

The background of the cover is a dark, futuristic digital space. It features glowing blue and cyan light trails, circular patterns, and a central bright light source that creates a lens flare effect. The overall aesthetic is high-tech and cybernetic.

Bitdefender®

GravityZone

ADMINISTRATORHANDBUCH

Bitdefender GravityZone Administratorhandbuch

Veröffentlicht 2021.04.20

Copyright© 2021 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuchs dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr“ gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokument entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte oder von Bitdefender kontrollierte Webseiten und somit übernimmt Bitdefender auch keine Verantwortung für die Inhalte dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Inhaltsverzeichnis

- Vorwort viii
 - 1. In diesem Handbuch verwendete Konventionen viii
- 1. Über GravityZone 1
- 2. GravityZone-Sicherheitsebenen 2
 - 2.1. Malware-Schutz 2
 - 2.2. Advanced Threat Control 4
 - 2.3. HyperDetect 4
 - 2.4. Erweiterter Exploit-Schutz 4
 - 2.5. Firewall 5
 - 2.6. Inhalts-Steuerung 5
 - 2.7. Network Attack Defense 5
 - 2.8. Patch-Verwaltung 5
 - 2.9. Gerätesteuerung 6
 - 2.10. Full Disk Encryption 6
 - 2.11. Security for Exchange 6
 - 2.12. Anwendungssteuerung 7
 - 2.13. Sandbox Analyzer 7
 - 2.14. Hypervisor Memory Introspection (HVI) 7
 - 2.15. Network Traffic Security Analytics (NTSA) 8
 - 2.16. Security for Storage 9
 - 2.17. Security for Mobile 9
 - 2.18. Verfügbarkeit der GravityZone-Sicherheitsebenen 10
- 3. GravityZone-Architektur 11
 - 3.1. GravityZone VA 11
 - 3.1.1. GravityZone-Datenbank 12
 - 3.1.2. GravityZone-Update-Server 12
 - 3.1.3. GravityZone-Kommunikationsserver 12
 - 3.1.4. Web-Konsole (GravityZone Control Center) 12
 - 3.1.5. Report-Builder-Datenbank 12
 - 3.1.6. Berichterstellungs-Verarbeitungsmodule 13
 - 3.2. Security Server 13
 - 3.3. HVI-Ergänzungspaket 13
 - 3.4. Sicherheitsagenten 13
 - 3.4.1. Bitdefender Endpoint Security Tools 14
 - 3.4.2. Endpoint Security for Mac 16
 - 3.4.3. GravityZone Mobile Client 16
 - 3.4.4. Bitdefender Tools (vShield) 17
 - 3.5. Sandbox Analyzer-Architektur 17
- 4. Erste Schritte 20
 - 4.1. Verbinden mit dem Control Center 20
 - 4.2. Control Center auf einen Blick 21
 - 4.2.1. Übersicht über die Control Center 21
 - 4.2.2. Tabellendaten 23



4.2.3. Symboleleisten	24
4.2.4. Kontextmenü	25
4.2.5. Ansichtsauswahl	25
4.3. Verwalten Ihres Kontos	26
4.4. Ändere Login Passwort	29
5. Benutzerkonten	30
5.1. Benutzerrollen	31
5.2. Benutzerrechte	33
5.3. Benutzerkonten verwalten	33
5.3.1. Einzelverwaltung von Benutzerkonten	34
5.3.2. Verwaltung mehrerer Benutzerkonten	37
5.4. Anmeldepasswörter zurücksetzen	41
5.5. Zwei-Faktor-Authentifizierung verwalten	41
6. Netzwerkobjekte verwalten	44
6.1. Mit Netzwerkansichten arbeiten	46
6.1.1. Computer und virtuelle Maschinen	46
6.1.2. Virtuelle Maschinen	47
6.1.3. Mobilgeräte	48
6.2. Computer	49
6.2.1. Überprüfen Sie den Status des Computers	50
6.2.2. Anzeigen von Computerdetails	53
6.2.3. Computer in Gruppen organisieren	67
6.2.4. Sortieren, Filtern und Suchen von Computern	69
6.2.5. Aufgaben ausführen	72
6.2.6. Schnellberichte erstellen	106
6.2.7. Richtlinien zuweisen	106
6.2.8.	107
6.2.9. Synchronisation mit Active Directory	108
6.3. Virtuelle Maschinen	109
6.3.1. Status virtueller Maschinen überprüfen	111
6.3.2. Details virtueller Maschinen anzeigen	114
6.3.3. Virtuelle Maschinen in Gruppen organisieren	123
6.3.4. Sortieren, Filtern und Suchen von virtuellen Maschinen	125
6.3.5. Aufgaben auf virtuellen Maschinen ausführen	130
6.3.6. Schnellberichte erstellen	168
6.3.7. Richtlinien zuweisen	169
6.3.8. Der Wiederherstellungsmanager für verschlüsselte Laufwerke	171
6.3.9. Freigeben von Lizenzplätzen	172
6.4. Mobilgeräte	172
6.4.1. Benutzerdefinierte Benutzer hinzufügen	173
6.4.2. Benutzern Mobilgeräte hinzufügen	175
6.4.3. Benutzerdefinierte Benutzer in Gruppen organisieren	177
6.4.4. Status der Mobilgeräte überprüfen	179
6.4.5. Konforme und Nicht-konforme Geräte	181
6.4.6. Details zu Benutzern und Mobilgeräten anzeigen	182
6.4.7. Sortieren, Filtern und Suchen von Mobilgeräten	185
6.4.8. Aufgaben auf Mobilgeräten ausführen	190

6.4.9. Schnellberichte erstellen	195
6.4.10. Richtlinien zuweisen	196
6.4.11. Synchronisation mit Active Directory	197
6.4.12. Benutzer und Mobilgeräte löschen	197
6.5. Anwendungsbestand	199
6.6. Patch-Inventar	205
6.6.1. Anzeigen von Patch-Informationen	206
6.6.2. Suchen und Filtern von Patches	207
6.6.3. Ignorieren von Patches	208
6.6.4. Installieren von Patches	209
6.6.5. Deinstallieren von Patches	211
6.6.6. Patch-Statistiken erstellen	213
6.7. Aufgaben anzeigen und verwalten	214
6.7.1. Aufgabenstatus überprüfen	214
6.7.2. Aufgabenberichte anzeigen	216
6.7.3. Aufgaben werden neu gestartet	217
6.7.4. Anhalten von Exchange-Scan-Aufgaben	217
6.7.5. Aufgaben löschen	218
6.8. Endpunkte aus dem Netzwerkinventar löschen	218
6.9. Konfigurieren von Netzwerkeinstellungen	219
6.9.1. Netzwerkinventareinstellungen	220
6.9.2. Offline-Maschinen-Bereinigung	220
6.10. Konfigurieren von Security Server-Einstellungen	222
6.11. Zugangsdaten-Manager	223
6.11.1. Betriebssystem	224
6.11.2. Virtuelle Umgebung	225
6.11.3. Zugangsdaten aus dem Zugangsdaten-Manager löschen	226
7. Sicherheitsrichtlinien	227
7.1. Policies verwalten	228
7.1.1. Richtlinien erstellen	229
7.1.2. Richtlinien zuweisen	231
7.1.3. Richtlinieneinstellungen ändern	242
7.1.4. Richtlinien umbenennen	243
7.1.5. Richtlinien löschen	243
7.2. Richtlinien für Computer und virtuelle Maschinen	244
7.2.1. Allgemein	245
7.2.2. HVI	260
7.2.3. Malware-Schutz	269
7.2.4. Sandbox Analyzer	312
7.2.5. Firewall	320
7.2.6. Netzwerkschutz	335
7.2.7. Patch-Verwaltung	351
7.2.8. Anwendungssteuerung	355
7.2.9. Gerätesteuerung	360
7.2.10. Relais	366
7.2.11. Exchange-Schutz	368
7.2.12. Verschlüsseln	401
7.2.13. NSX	406

7.2.14. Speicherschutz	406
7.3. Richtlinien für Mobilgeräte	410
7.3.1. Allgemein	411
7.3.2. Geräteverwaltung	411
8. Überwachungs-Dashboard	434
8.1. Dashboard	434
8.1.1. Portlet-Daten neu laden	435
8.1.2. Portlet-Einstellungen bearbeiten	436
8.1.3. Ein neues Portlet hinzufügen	436
8.1.4. Ein Portlet entfernen	436
8.1.5. Portlets neu anordnen	436
9. Berichte verwenden	438
9.1. Berichtstypen	438
9.1.1. Berichte zu Computern und virtuellen Maschinen	439
9.1.2. Exchange-Server-Berichte	454
9.1.3. Berichte zu Mobilgeräten	457
9.2. Berichte erstellen	459
9.3. Geplante Berichte anzeigen und verwalten	463
9.3.1. Berichte betrachten	464
9.3.2. Geplante Berichte bearbeiten	465
9.3.3. Geplante Berichte löschen	466
9.4. Berichtsbasierte Aktionen ausführen	466
9.5. Berichte speichern	467
9.5.1. Berichte exportieren	468
9.5.2. Berichte herunterladen	468
9.6. Berichte per E-Mail versenden	468
9.7. Berichte ausdrucken	469
9.8. Report-Builder	469
9.8.1. Abfragetypen	470
9.8.2. Abfragen verwalten	471
9.8.3. Berichte anzeigen und verwalten	478
10. Quarantäne	481
10.1. Die Quarantäne im Detail	481
10.2. Quarantäne für Computer und virtuelle Maschinen	482
10.2.1. Quarantäne-Details anzeigen	483
10.2.2. Verwalten von Dateien in der Quarantäne	483
10.3. Exchange-Server-Quarantäne	488
10.3.1. Quarantäne-Details anzeigen	488
10.3.2. In die Quarantäne verschobene Objekte	490
11. Verwenden des Sandbox Analyzers	495
11.1. Filtern von Übermittlungskarten	496
11.2. Anzeigen von Analysedetails	498
11.3. Erneute Übermittlung von Stichproben	499
11.4. Löschen von Übermittlungskarten	501
11.5. Manuelle Übermittlung	501
11.6. Verwalten der Sandbox Analyzer-Infrastruktur	504

11.6.1. Überprüfen des Sandbox Analyzer-Status	504
11.6.2. Konfigurieren gleichzeitiger Detonationen	506
11.6.3. Überprüfen des Status des VM-Images	507
11.6.4. Konfigurieren und Verwalten von VM-Images	508
12. Benutzeraktivitätsprotokoll	509
13. Verwendung von Tools	511
13.1. Benutzerdefiniert Tool-Injektion mit HVI	511
14. Benachrichtigungen	513
14.1. Benachrichtigungsarten	513
14.2. Benachrichtigungen anzeigen	522
14.3. Benachrichtigungen löschen	523
14.4. Benachrichtigungseinstellungen konfigurieren	523
15. Systemstatus	527
15.1. Status OK	528
15.2. Status Achtung	528
15.3. Metriken	529
16. Hilfe erhalten	532
16.1. Bitdefender-Support-Center	532
16.2. Hilfe anfordern	534
16.3. Verwenden des Support-Tools	534
16.3.1. Das Support-Tool unter Windows verwenden	534
16.3.2. Das Support-Tool unter Linux	536
16.3.3. Das Support-Tool unter Mac verwenden	537
16.4. Kontaktinformation	538
16.4.1. Internet-Adressen	538
16.4.2. Händler vor Ort	539
16.4.3. Bitdefender-Niederlassungen	539
A. Anhänge	542
A.1. Unterstützte Dateitypen	542
A.2. Netzwerkobjekttypen und -status	543
A.2.1. Netzwerkobjekttypen	543
A.2.2. Netzwerkobjektstatus	544
A.3. Anwendungsdateitypen	545
A.4. Dateitypen für die Anhangsfilterung	546
A.5. Systemvariablen	546
A.6. Tools der Anwendungssteuerung	548
A.7. Sandbox Analyzer-Objekte	549
A.7.1. Unterstützte Dateitypen und Dateieindungen für die manuelle Übermittlung	549
A.7.2. Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden	550
A.7.3. Standardausschlüsse bei automatischer Übermittlung	550
A.7.4. Empfohlene Anwendungen für die Detonations-VMs	550
A.8. Datenprozessoren	551
Glossar	555

Vorwort

Dieses Handbuch richtet sich an Netzwerkadministratoren, die mit der Verwaltung von GravityZone innerhalb ihres Unternehmens betraut sind.

In diesem Dokument wird beschrieben, wie Sie mit dem GravityZone Control Center Sicherheitseinstellungen auf Endpunkten unter Ihrem Konto anzeigen und konfigurieren können. Hier erfahren Sie, wie Sie Ihr Netzwerkinventar in Control Center anzeigen, Richtlinien erstellen und auf verwalteten Endpunkten anwenden sowie Berichte erstellen, Objekte in der Quarantäne verwalten und das Dashboard nutzen.

1. In diesem Handbuch verwendete Konventionen

Typografie

In diesem Handbuch werden zur besseren Lesbarkeit verschiedene Schriftarten verwendet. In der unten stehenden Tabelle erfahren Sie, was welche Schriftart bedeutet.

Erscheinungsbild	Beschreibung
Beispiel	Eingebende Befehle und Syntaxen, Pfade und Dateinamen, Konfigurationen, Dateiausgaben und andere Eingabetexte sind in nicht-proportionaler Schrift gedruckt.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
gravityzone-docs@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. viii)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Produktoptionen werden fett gedruckt dargestellt.
Stichwort	Optionen der Benutzeroberfläche, Stichwörter oder Tastenkombinationen werden durch Fettdruck hervorgehoben.

Hinweise

Hierbei handelt es sich um Hinweise innerhalb des Textflusses, welche mit einer kleinen Grafik markiert sind. Es handelt sich um Informationen, die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten in der Regel nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden wichtige Informationen zum jeweiligen Thema gegeben, die nicht übersprungen werden sollten.



Warnung

Diese kritische Information erfordert größtmögliche Aufmerksamkeit. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst kritische Thematik handelt.

1. ÜBER GRAVITYZONE

GravityZone ist eine Sicherheitslösung für Unternehmen, die speziell auf virtuelle und Cloud-Umgebungen zugeschnitten ist, und bietet Sicherheitsdienste für physische Endpunkte, Mobilgeräte und virtuelle Maschinen in der Private und der Public Cloud sowie für Exchange-Mail-Server.

GravityZone ist ein umfassendes Produkt mit einer zentralen Verwaltungskonsole, die entweder von Bitdefender in der Cloud gehostet oder als virtuelle Appliance innerhalb des Unternehmens installiert wird. Über diese Konsole können von zentraler Stelle aus Sicherheitsrichtlinien für eine beliebige Zahl an Endpunkten erstellt, zugewiesen und verwaltet werden, unabhängig vom Typ und geographischen Ort dieser Endpunkte.

GravityZone bietet Sicherheit für Endpunkte und Microsoft-Exchange-Mail-Server in mehreren Schichten: Malware-Schutz mit Verhaltensüberwachung, Schutz vor Zero-Day-Attacks, Anwendungssteuerung und Sandboxing, Firewall, Gerätesteuerung, Inhaltssteuerung sowie Phishing- und Spam-Schutz.

2. GRAVITYZONE-SICHERHEITSEBENEN

GravityZone umfasst die folgenden Sicherheitsebenen:

- Malware-Schutz
- Advanced Threat Control
- HyperDetect
- Erweiterter Exploit-Schutz
- Firewall
- Inhalts-Steuerung
- Patch-Verwaltung
- Gerätesteuerung
- Full Disk Encryption
- Security for Exchange
- Anwendungssteuerung
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Malware-Schutz

Das Anti-Malware-Sicherheitsebene setzt Signatur-Scans und heuristische Analysen (B-HAVE, ATC) ein, um Schutz vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und anderer bössartiger Software zu gewährleisten.

Bitdefenders Malware-Scans setzen auf die folgenden Technologien:

- Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der Signaturdatenbank abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt sehr effektiv bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat.
- Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische

Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt verdächtige Dateien in einer virtuellen Umgebung aus, um ihre Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.

Scan-Engines

Bitdefender GravityZone ist in der Lage, die Scan-Engines beim Erstellen der Pakete für die Sicherheitsagenten entsprechend der Endpunktkonfiguration automatisch anzupassen.

Administratoren können die Scan-Engines auch manuell anpassen. Dabei können sie unter den folgenden Optionen wählen:

1. **Lokaler Scan:** für Scans, die auf lokalen Endpunkten durchgeführt werden. Der lokale Scan-Modus eignet sich für leistungsstarke Maschinen, auf denen alle Signaturen und Engines lokal gespeichert sind.
2. **Hybrid-Scan mit leichten Engines (Public Cloud):** mittlerer Ressourcenverbrauch; gescannt wird in der Cloud und zum Teil auch mithilfe lokaler Signaturen. Dieser Scan-Modus reduziert den Ressourcenverbrauch durch Auslagerung der Scan-Aktivität.
3. **Zentralisierter Scan in der Public oder Private Cloud:** geringer Ressourcenverbrauch; benötigt einen Security Server zum Scan. In diesem Fall werden keine Signaturen lokal gespeichert. Die Scan-Aktivität wird auf den Security Server ausgelagert.



Beachten Sie

Es gibt eine Mindestanzahl an lokal gespeicherten Engines, die zum Entpacken der komprimierten Dateien benötigt werden.

4. **Zentralisierter Scan (Scan in der Public oder Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Full Engines)**
5. **Zentralisierter Scan (Scan in der Public oder Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (Public Cloud mit leichten Engines)**

* Bei Scans mit zwei Engines wird die Ausweich-Engine verwendet, wenn die erste Engine nicht verfügbar ist. Der Ressourcenverbrauch und die Netzwerknutzung hängen von den verwendeten Engines ab.

2.2. Advanced Threat Control

Für Bedrohungen, die selbst von der heuristischen Engine nicht erkannt werden, wurde mit Advanced Threat Control (ATC) eine weitere Sicherheitsebene eingerichtet.

Advanced Threat Control überwacht ununterbrochen laufende Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel Verbergen des Prozessstyps, Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, Ablegen von Dateien, Verbergen vor Anwendungen zur Prozessübersicht usw. Jedes verdächtige Verhalten steigert den Verdachtswert des Prozesses. Bei Überschreiten einer Schwelle wird ein Alarm ausgelöst.

2.3. HyperDetect

Bitdefender HyperDetect ist eine zusätzliche Sicherheitsebene, die speziell entwickelt wurde, um komplexe Angriffe und verdächtige Aktivitäten noch vor der Ausführungsphase zu erkennen. HyperDetect enthält maschinelle Lernmodelle und Technologien zur Erkennung von getarnten Angriffen zur Abwehr von Bedrohungen wie Zero-Day-Angriffen, Advanced Persistent Threats (APT), verschleierte Malware, dateilosen Angriffen (Missbrauch von PowerShell, Windows Management Instrumentation usw.), Diebstahl von Anmeldeinformationen, gezielten Angriffen, Custom Malware, skriptbasierten Angriffen, Exploits, Hacking-Tools, verdächtigem Netzwerkverkehr, potenziell unerwünschten Anwendungen (PUA) und Ransomware.



Beachten Sie

Dieses Modul ist ein Add-on, das mit einem eigenen Lizenzschlüssel erhältlich ist.

2.4. Erweiterter Exploit-Schutz

Diese neue proaktive Technologie nutzt maschinelle Lernverfahren und stoppt so Zero-Day-Angriffe, die nur schwer zu findende Exploits ausnutzen. Der erweiterte Exploit-Schutz findet auch die neuesten Exploits in Echtzeit und behebt Memory-Corruption-Schwachstellen, die vorhandene Sicherheitslösungen umgehen können. Schützt die gebräuchlichsten Anwendungen, wie Browser, Microsoft Office oder Adobe Reader, sowie andere, die Ihnen einfallen. Überwacht Systemprozesse und schützt vor Sicherheitseinbrüchen und Prozess-Hijacking.

2.5. Firewall

Die Firewall steuert den Zugriff von Anwendungen auf das Netzwerk sowie auf das Internet. Eine umfangreiche Datenbank enthält eine Liste bekannter, vertrauenswürdiger Anwendungen, denen automatisch Zugriff gewährt wird. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.

2.6. Inhalts-Steuerung

Mit dem Modul Inhaltssteuerung können Unternehmensrichtlinien für zugelassenen Datenverkehr, Internetzugriff, Datenschutz und Anwendungssteuerung durchgesetzt werden. Administratoren können Scan-Optionen und -Ausschlüsse für den Datenverkehr festlegen, den Internetzugriff auf bestimmte Zeiten beschränken, einzelne Internetkategorien oder URLs blockieren, Identitätsschutzregeln konfigurieren und Rechte für die Verwendung bestimmter Anwendungen festlegen.

2.7. Network Attack Defense

Das Network Attack Defense-Modul nutzt eine Bitdefender-Technologie zur Erkennung von Angriffen auf das Netzwerk, mit denen versucht wird, über Verfahren wie Brute-Force-Angriffe, Netzwerk-Exploits, Passwortdiebstahl, Drive-by-Download-Infektionsvektoren, Bots oder Trojaner Zugriff auf Endpunkte zu erlangen.

2.8. Patch-Verwaltung

Die Patch-Verwaltung ist vollständig in GravityZone integriert und sorgt dafür, dass Ihre Programme und Ihr Betriebssystem immer auf dem neuesten Stand sind und verleiht Ihnen einen Überblick über den Patch-Status der verwalteten Windows-Endpunkte.

Das GravityZone-Modul Patch-Verwaltung beinhaltet verschiedene Funktionen, darunter Patch-Scans auf Knopfdruck oder nach Plan, automatische/manuelle Aufspielung von Patches und Berichte zu fehlenden Patches.

Welche Anbieter und Produkte von der GravityZone-Patch-Verwaltung unterstützt werden, können Sie in [Artikel](#) nachlesen.

**Beachten Sie**

Die Patch-Verwaltung ist ein Add-on, das über einen separaten Lizenzschlüssel für alle GravityZone-Pakete erworben werden kann.

2.9. Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und -Ausnahmen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine Vielzahl von Gerätearten möglich wie zum Beispiel USB-Sticks, Bluetooth-Geräte, CD/DVD-Player, Speichermedien und vieles mehr.

2.10. Full Disk Encryption

Diese Sicherheitsebene verwaltet BitLocker unter Windows sowie FileVault und diskutil unter macOS und ermöglicht so eine vollständige Festplattenverschlüsselung auf Ihren Endpunkten. Sie können bootfähige und nicht bootfähige Laufwerke mit nur einem Klick verschlüsseln und entschlüsseln. Dabei übernimmt GravityZone die meiste Arbeit. Sie selbst müssen kaum etwas tun. Außerdem werden in GravityZone die Wiederherstellungsschlüssel gespeichert, die zur Entschlüsselung der Laufwerke benötigt werden, falls der Benutzer mal das Passwort vergessen sollte.

**Beachten Sie**

Die Full Disk Encryption ist ein Add-on, das über einen separaten Lizenzschlüssel für alle GravityZone-Pakete erworben werden kann.

2.11. Security for Exchange

Bitdefender Security for Exchange bietet Malware-, Spam- und Phishing-Schutz sowie eine Anhang- und Inhaltsfilterung. Die Lösung lässt sich nahtlos mit Microsoft Exchange Server integrieren und schafft so eine Malware-freie E-Mail- und Kollaborationsumgebung und erhöht damit die Produktivität. Dank mehrfach ausgezeichneten Malware- und Spam-Schutz-Technologie schützt die Software Exchange-Benutzer selbst vor raffinierter, bisher unbekannter Malware sowie vor Datendiebstahl.

**Wichtig**

Security for Exchange wurde entwickelt, um die gesamte Exchange-Organisation zu schützen, zu der der geschützte Exchange-Server gehört. Das bedeutet, dass es alle

aktiven Postfächer schützt, einschließlich Benutzer-,Raum-,Geräte- und freigegebene Postfächer.

Zusätzlich zum Microsoft Exchange-Schutz umfasst die Lizenz die auf dem Server installierten Module für den Endpunktschutz.

2.12. Anwendungssteuerung

Das Anwendungssteuerungsmodul verhindert Malware- und Zero-Day-Angriffe und sorgt für zuverlässige Sicherheit, ohne die Mitarbeiterproduktivität zu beeinträchtigen. Mit der Anwendungssteuerung können flexible Richtlinien für das Whitelisting von Anwendungen angewandt werden, die eine Installation und Ausführung von nicht erwünschten, nicht vertrauenswürdigen oder schädlichen Anwendungen erkennen und verhindern.

2.13. Sandbox Analyzer

Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben. In der Sandbox kommen verschiedene Bitdefender-Technologien zum Einsatz, mithilfe derer Schadcode in einer abgeschlossenen, von Bitdefender gehosteten virtuellen Umgebung ausgeführt, anschließend das Verhalten analysiert und jede noch so kleine Veränderung am System, die auf schädliche Aktivitäten hindeuten könnten, gemeldet wird.

Sandbox Analyzer verwendet eine Reihe von Sensoren, um Inhalte von verwalteten Endpunkten, aus Netzwerk-Datenströmen, der zentralen Quarantäne und ICAP-Servern zu detonieren.

Darüber hinaus ermöglicht Sandbox Analyzer die manuelle Übermittlung von Proben und die Übermittlung über die API.

2.14. Hypervisor Memory Introspection (HVI)

Es ist allgemein bekannt, dass durchorganisierte, profitorientierte Angriffe unerkannte Sicherheitslücken (Zero-Day-Lücken) suchen oder einmalige, zweckgerichtete Exploits (Zero-Day-Exploits) und andere Mittel nutzen. Angreifer verwenden zudem hochentwickelte Techniken, mit denen sie Angriffe verzögern oder fragmentieren, um sicherheitsgefährdende Aktivitäten zu verschleiern.

Profitorientierte Angriffe jüngerer Datums sind getarnt und umgehen traditionelle Sicherheits-Tools.

Für virtualisierte Umgebungen ist das Problem nun behoben, da HVI Datenzentren mit hoher Dichte an virtuellen Maschinen vor hochentwickelten, fortschrittlichen Bedrohungen schützt, die signatur-basierte Engines nicht bekämpfen können. Es bietet hohe Abschirmung, erkennt Angriffe in Echtzeit und wehrt sie direkt beim Auftreten ab und schaltet die Bedrohung aus.

Ob es sich um ein Windows- oder Linuxgerät, um einen Server oder einen Arbeitsplatzrechner handelt, HVI bietet Einblick in einem Umfang, der aus Sicht des Gast-Betriebssystems nicht möglich ist. So wie der Hypervisor den Hardware-Zugang für alle virtuellen Gast-Maschinen kontrolliert, verfügt HVI über Detailwissen hinsichtlich Benutzermodus und Betriebssystem (Kernel Mode) des Gastspeichers. Folglich hat HVI vollständigen Einblick in den Gastspeicher und somit ein umfassendes Gesamtbild. Gleichzeitig ist HVI vom geschützten Gast isoliert im gleichen Maße wie der Hypervisor selbst isoliert ist. Da HVI auf Hypervisor-Ebene arbeitet und die Hypervisor-Funktionalitäten unterstützt, bewältigt es die technischen Herausforderungen traditioneller Sicherheitssysteme und deckt so bösartige Aktivitäten in Datenzentren auf.

HVI erkennt nicht Angriffsmuster, sondern Angriffstechniken. So kann diese Technologie übliche Exploit-Techniken erkennen, melden und verhindern. Der Kernel ist gegen Rootkit-Hook-Techniken geschützt, die während des Angriffs als Tarnung verwendet werden. Benutzer-Modus-Vorgänge sind außerdem gegen Code-Injection, Function-Detour und Code-Ausführung aus dem Stapel- oder Heap-Speicher geschützt.

2.15. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) ist eine Lösung für die Netzwerksicherheit, die IPFIX-Datenverkehrsströme auf böses Verhalten und Malware überprüft.

Bitdefender NTSA soll neben Ihren bestehenden Sicherheitsmaßnahmen als ergänzender Schutz dienen, der in der Lage ist, auch tote Winkel abzudecken, die herkömmliche Tools nicht überwachen.

Herkömmliche Tools für die Netzwerksicherheit versuchen in der Regel, Malware-Infektionen zu verhindern, indem sie den eingehenden Datenverkehr überprüfen (über Sandbox, Firewall, Virenschutzprogramme usw.). Bitdefender

NTSA konzentriert sich ausschließlich auf die Überwachung des ausgehenden Netzwerkverkehrs auf bösartiges Verhalten.

2.16. Security for Storage

Mit GravityZone Security for Storage erhalten Sie erstklassigen Echtzeitschutz für alle führenden File-Sharing- und Netzwerkspeichersysteme. Alle Upgrades des Systems und der Algorithmen für die Bedrohungserkennung laufen automatisch ab. Dadurch entstehen Ihnen keine Aufwände und Ihre Nutzer werden nicht in ihrer Arbeit gestört.

Zwei oder mehrere GravityZone Security Server Multi-Platform übernehmen die Rolle des ICAP-Servers, über den die Dienste für den Malware-Schutz für ICAP-konforme (siehe RFC3507) Network-Attached-Storage-Geräte (NAS) und File-Sharing-Systeme bereitgestellt werden.

Sobald ein Benutzer über seinen Laptop, seinen Arbeitsplatzrechner, sein Mobilgerät oder ein anderes Gerät eine Anfrage zum Öffnen, Lesen, Schreiben oder Schließen einer Datei stellt, übermittelt der ICAP-Client (NAS- oder File-Sharing-System) ein Scan-Anfrage an den Security Server und erhält eine entsprechende Rückinformation. Davon abhängig erlaubt der Security Server den Zugriff, verweigert den Zugriff oder löscht die Datei.



Beachten Sie

Dieses Modul ist ein Add-on, das mit einem eigenen Lizenzschlüssel erhältlich ist.

2.17. Security for Mobile

Die Lösung vereint unternehmensweite Sicherheit mit der Verwaltung und Compliance-Überwachung von iPhones, iPads und Android-Geräten durch die zuverlässige Bereitstellung von Software und Updates über die Apple- und Android-Marktplätze. Durch einheitliche Durchsetzung von Sicherheitsrichtlinien auf allen Mobilgeräten können Mitarbeiter ihre eigenen Geräte sicher und kontrolliert im Unternehmensnetzwerk verwenden (BYOD). Zu den Sicherheitsfunktionen gehören Bildschirm Sperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht. So werden die Mobilgeräte zuverlässig kontrolliert und die darauf gespeicherten sensiblen Unternehmensdaten geschützt.

2.18. Verfügbarkeit der GravityZone-Sicherheitsebenen

Die Verfügbarkeit der verschiedenen GravityZone-Sicherheitsebenen hängt vom Betriebssystem des Endpunkts ab. Weitere Informationen finden Sie in der Wissensdatenbank im Artikel [Verfügbarkeit der GravityZone-Sicherheitsebenen](#).

3. GRAVITYZONE-ARCHITEKTUR

Dank seiner einzigartigen Architektur ist GravityZone extrem skalierbar und kann eine beliebige Anzahl von Systemen schützen. GravityZone kann mehrere virtuelle Appliances und mehrere Instanzen bestimmter Rollen (Datenbank, Kommunikationsserver, Update-Server und Web-Konsole) verwenden, um Verfügbarkeit und Skalierbarkeit auf hohem Niveau zu halten.

Jede Instanz einer Rolle kann auf einer anderen Appliance installiert werden. Eingebaute Lastenverteilungen gewährleisten, dass GravityZone selbst die umfangreichsten Unternehmensnetzwerke zuverlässig schützen kann, ohne Verzögerungen oder Ressourcenengpässe zu verursachen. Statt der eingebauten Lastenverteilungen kann auch Drittanbieter-Software zur Lastenverteilung eingesetzt werden.

GravityZone wird als virtueller Container zur Verfügung gestellt und kann so in jede virtuelle Umgebung importiert werden, egal ob sie mit VMware, Citrix, Microsoft Hyper-V, Nutanix Prism oder Microsoft Azure betrieben wird.

Die Integration mit VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element und Microsoft Azure macht es leichter, physische und virtuelle Endpunkte gleichzeitig zu schützen.

GravityZone besteht aus den folgenden Komponenten:

- [GravityZone-Virtual-Appliance](#)
- [Security Server](#)
- [HVI-Ergänzungspaket](#)
- [Sicherheitsagenten](#)

3.1. GravityZone VA

In der On-Premises-Version wird GravityZone als selbst-konfigurierende virtuelle Hochsicherheits-Linux-Ubuntu-Appliance (VA) zur Verfügung gestellt, die in einem virtuellen Maschinen-Image eingebettet ist und unkompliziert über eine Befehlszeilenoberfläche installiert und konfiguriert werden kann. Die virtuelle Appliance steht in verschiedenen Formaten zur Verfügung, die mit allen gängigen Virtualisierungsplattformen kompatibel sind (OVA, XVA, VHD, OVF, RAW).

3.1.1. GravityZone-Datenbank

Die zentrale Logik der GravityZone-Architektur. Bitdefender setzt eine nicht-relationale MongoDB-Datenbank ein, um Skalierung und Replikation zu erleichtern.

3.1.2. GravityZone-Update-Server

Der Update-Server übt die wichtige Funktion aus, die GravityZone und die Endpunkt-Agenten auf dem neuesten Stand zu halten, indem er die nötigen Pakete oder Installationsdateien repliziert und veröffentlicht.

3.1.3. GravityZone-Kommunikationsserver

Der Kommunikationsserver stellt das Bindeglied zwischen den Sicherheitsagenten und der Datenbank dar. Er übermittelt Richtlinien und Aufgaben an geschützte Endpunkte sowie die von Sicherheitsagenten gemeldeten Ereignisse.

3.1.4. Web-Konsole (GravityZone Control Center)

Die Sicherheitslösungen in Bitdefender werden über die Control Center-Web-Konsole von zentraler Stelle aus verwaltet. Dies erleichtert die Verwaltung und den Zugriff auf die allgemeine Sicherheitslage sowie auf globale Sicherheitsrisiken und ermöglicht zudem die zentrale Steuerung der Sicherheitsdienste, die virtuelle und physische Arbeitsplatzrechner, Server und Mobilgeräte schützen. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst größter Unternehmen zu erfüllen.

Das Control Center lässt sich mit den bestehenden Systemverwaltungs- und Überwachungssystemen integrieren und macht es damit einfacher, nicht verwaltete Arbeitsplatzrechner, Server und Mobilgeräte automatisch zu schützen, die in Microsoft Active Directory, VMware vCenter, Nutanix Prism Element oder Citrix XenServer aufgeführt werden oder einfach im Netzwerk gefunden werden.

3.1.5. Report-Builder-Datenbank

Die Rolle Report-Builder-Datenbank stellt die nötigen Daten für die Erstellung abfragebasierter Berichte zur Verfügung.

3.1.6. Berichterstellungs-Verarbeitungsmodule

Die Report-Builder-Prozessorenrolle ist essenziell für die Erstellung, Verwaltung und Speicherung der abfragebasierten Berichte, die Informationen aus der Report-Builder-Datenbank verwenden.

3.2. Security Server

Security Server ist eine virtuelle Maschine, die eigens für die Deduplizierung und Zentralisierung eines Großteils der Malware-Schutzfunktionen der Malware-Schutz-Agenten entwickelt wurde und als Scan-Server fungiert.

Es gibt drei Security Server-Versionen für jeden Typ von Virtualisierungsumgebung:

- **Security Server for VMware NSX.** Diese Version wird automatisch auf jedem Host im Cluster installiert, auf dem Bitdefender bereitgestellt wurde.
- **Security Server für VMware vShield-Endpoint.** Diese Version muss auf jedem Host installiert sein, der geschützt werden soll.
- **Security Server Multi-Plattform.** Diese Version ist für verschiedene andere virtualisierte Umgebungen gedacht und muss auf einem oder mehreren Hosts installiert sein, um die gewünschte Anzahl an virtuellen Maschinen gewährleisten zu können. Bei Verwendung von HVI muss ein Security Server auf jedem Host installiert sein, der zu schützende virtuelle Maschinen enthält.

3.3. HVI-Ergänzungspaket

Das HVI-Paket stellt die Verbindung zwischen Hypervisor und dem Security Server auf diesem Host sicher. So ist der Security Server in der Lage, den Speicher des Hosts, auf dem er installiert ist, unter Beachtung der GravityZone-Sicherheitsrichtlinien zu überwachen.

3.4. Sicherheitsagenten

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die entsprechenden GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren.

- [Bitdefender Endpoint Security Tools](#)
- [Endpoint Security for Mac](#)
- [GravityZone Mobile Client](#)
- [Bitdefender Tools \(vShield\)](#)

3.4.1. Bitdefender Endpoint Security Tools

GravityZone stellt den Schutz physischer und virtueller Maschinen unter Windows und Linux mit Bitdefender Endpoint Security Tools sicher. Dabei handelt es sich um einen intelligenten Sicherheitsagenten, der die Umgebung, in der er eingesetzt wird, erkennt, und sich entsprechend an die Ressourcen des Endpunkttyps anpasst. Bitdefender Endpoint Security Tools kann sowohl auf virtuellen und physischen Computern bereitgestellt werden und stellt ein flexibles Scan-System zur Verfügung, das es zur perfekten Wahl für heterogene Umgebungen (physisch, virtuell und Cloud) macht.

Bitdefender Endpoint Security Tools schützt nicht nur das Dateisystem, sondern auch Microsoft-Exchange-Mail-Server.

Bitdefender Endpoint Security Tools benötigt nur eine einzige Richtlinienvorlage für physische und virtuelle Maschinen und nur ein einziges Installationskit für physische und virtuelle Umgebungen mit Windows.

Schutzebenen

Die folgenden Sicherheitsebenen stehen in Bitdefender Endpoint Security Tools zur Verfügung:

- Malware-Schutz
- Advanced Threat Control
- HyperDetect
- Firewall
- Inhalts-Steuerung
- Network Attack Defense
- Patch-Verwaltung
- Gerätesteuerung
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Anwendungssteuerung

Endpunkttrollen

- Power-User
- Relais
- Patch-Cache-Server
- Exchange-Schutz

Power-User

Control-Center-Administratoren können über Richtlinieneinstellungen bestimmten Endpunkt-Benutzern Power-User-Rechte gewähren. Mit dem Power-User-Modul können Benutzern Administratorrechte verliehen werden, mit denen sie über die lokale Konsole Sicherheitseinstellungen anzeigen und verändern können. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.



Wichtig

Dieses Modul steht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung. Weitere Informationen hierzu finden Sie in der GravityZone-Installationsanleitung.

Relais

Endpunktagenten mit der Rolle Bitdefender Endpoint Security Tools Relay fungieren als Kommunikations-Proxy- und Update-Server für andere Endpunkte im Netzwerk. Endpunkt-Agenten mit Relais-Rolle werden besonders in Unternehmen mit isolierten Netzwerken benötigt, in denen sämtlicher Datenverkehr über einen einzelnen Zugangspunkt läuft.

In Unternehmen mit großen, geographisch dezentralen Netzwerken reduzieren Relais-Agenten die benötigte Bandbreite, indem sie verhindern, dass geschützte Endpunkte und Security Server eine direkte Verbindung zur GravityZone herstellen.

Nachdem ein Bitdefender Endpoint Security Tools Relay im Netzwerk installiert wurde, können andere Endpunkte per Richtlinie so konfiguriert werden, dass sie über den Relais-Agenten mit dem Control Center kommunizieren.

Bitdefender Endpoint Security Tools Relay-Agenten dienen den folgenden Zwecken:

- Alle ungeschützten Endpunkte im Netzwerk finden.
- Den Endpunkt-Agenten im lokalen Netzwerk installieren.
- Geschützte Endpunkte im Netzwerk auf dem neuesten Stand halten.
- Die Kommunikation zwischen dem Control Center und verbundenen Endpunkten gewährleisten.
- Als Proxy-Server für geschützte Endpunkte fungieren.
- Optimierung des Netzwerkverkehrs während der Durchführung von Updates, Installationen, Scan-Vorgängen und anderen ressourcenintensive Aufgaben.

Patch-Cache-Server

Endpunkte mit einer Relais-Rolle können auch als Patch-Cache-Server fungieren. Wird diese Rolle aktiviert, speichern die Relais die von den Anbieter-Websites heruntergeladenen Software-Patches und verteilen diese auf den Zielpunkten in Ihrem Netzwerk. Gibt es auf einem Endpunkt Software, für die ein Patch verfügbar ist, wird dieser Patch vom dem Server und nicht von der Anbieter-Website heruntergeladen. Dadurch entsteht weniger Datenverkehr und die Bandbreitenauslastung wird optimiert.



Wichtig

Diese zusätzliche Rolle ist mit einem registrierten Patch-Verwaltung-Add-on verfügbar.

Exchange-Schutz

Bitdefender Endpoint Security Tools mit Exchange-Rolle kann auf Microsoft-Exchange-Servern installiert werden, um Exchange-Benutzer vor per E-Mail übertragenen Gefahren zu schützen.

Bitdefender Endpoint Security Tools mit Exchange-Rolle schützt sowohl den Server selbst als auch die Lösung Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac ist ein Sicherheitsagent für Intel-basierte Macintosh-Computer und -Laptops. Die verfügbare Scan-Technologie ist **Lokaler Scan**; alle Sicherheitsinhalte werden dabei lokal gespeichert.

Schutzebenen

Die folgenden Sicherheitsebenen stehen in Endpoint Security for Mac zur Verfügung:

- [Malware-Schutz](#)
- [Advanced Threat Control](#)
- [Inhalts-Steuerung](#)
- [Gerätesteuerung](#)
- [Full Disk Encryption](#)

3.4.3. GravityZone Mobile Client

Mit GravityZone Mobile Client lassen sich Sicherheitsrichtlinien leicht auf eine beliebige Anzahl von Android- und iOS-Geräten anwenden und diese Geräte so vor unbefugtem Zugriff, Riskware und Datendiebstahl schützen. Zu den

Sicherheitsfunktionen gehören Bildschirmsperre, Authentifizierungskontrolle und Geräteortung, Datenlöschung per Fernzugriff und Erkennung von Geräten mit Root oder Jailbreak sowie Sicherheitsprofile. Auf Android-Geräten wird die Sicherheit noch einmal durch Echtzeit-Scans und die Verschlüsselung von Wechselmedien erhöht.

GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools ist ein leichter Agent für virtualisierte, mit vShield Endpoint integrierte VMware-Umgebungen. Der Sicherheitsagent wird auf virtuellen, durch Security Server geschützte Maschinen installiert und ermöglicht Ihnen die folgenden zusätzlichen Funktionalitäten:

- Ermöglicht Speicher- und Prozess-Scan-Aufgaben auf virtuellen Maschinen.
- Informiert den Benutzer über die gefundenen Infektionen und die daraufhin ausgeführten Aktionen.
- Fügt weitere Optionen für Anti-Malware-Scan-Ausschlüsse hinzu.

3.5. Sandbox Analyzer-Architektur

Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben.

Sandbox Analyzer ist in zwei Varianten erhältlich:

- [Sandbox Analyzer Cloud](#), von Bitdefender gehostet.
- [Sandbox Analyzer On-Premises](#), verfügbar als virtuelle Appliance, die lokal bereitgestellt werden kann.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud umfasst die folgenden Komponenten:

- **Sandbox Analyzer-Portal** – ein gehosteter Kommunikationsserver, der Anfragen zwischen Endpunkten und dem Bitdefender-Sandbox-Cluster bearbeitet.

- **Sandbox Analyzer-Cluster** – die gehostete Sandbox-Infrastruktur, innerhalb derer die virtuelle Verhaltensanalyse abläuft. Auf dieser Ebene werden die übermittelten Dateien auf virtuellen Maschinen unter Windows 7 ausgeführt.

Das **GravityZone Control Center** dient als Verwaltungs- und Berichtskonsole, über die Sicherheitsrichtlinien konfiguriert und Analyseberichte sowie Benachrichtigungen angezeigt werden können.

Bitdefender Endpoint Security Tools ist der auf Endpunkten installierte Sicherheitsagent, der als Einspeisungssensor für den Sandbox Analyzer fungiert.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises wird als virtuelle Linux Ubuntu-Appliance ausgeliefert, die in ein virtuelles Maschinen-Image eingebettet, einfach zu installieren und über eine Befehlszeilenschnittstelle (CLI) zu konfigurieren ist. Sandbox Analyzer On-Premises ist im OVA-Format verfügbar und kann auf VMWare ESXi installiert werden.

Eine Sandbox Analyzer On-Premises-Instanz umfasst die folgenden Komponenten:

- **Sandbox-Manager.** Diese Komponente ist der Sandbox-Orchestrator. Der Sandbox Manager verbindet sich über eine API mit dem ESXi-Hypervisor und nutzt seine Hardware-Ressourcen für den Aufbau und Betrieb der Malware-Analyse-Umgebung.
- **Virtuelle Maschinen für die Detonation.** Diese Komponente besteht aus virtuellen Maschinen, die von Sandbox Analyzer genutzt werden, um Dateien auszuführen und ihr Verhalten zu analysieren. Die virtuellen Maschinen für die Detonation können mit Windows 7 und Windows 10 64-Bit-Betriebssystemen betrieben werden.

Das **GravityZone Control Center** dient als Verwaltungs- und Berichtskonsole, über die Sicherheitsrichtlinien konfiguriert und Analyseberichte sowie Benachrichtigungen angezeigt werden können.

Sandbox Analyzer On-Premises nutzt die folgenden Einspeisungssensoren:

- **Endpunktsensor.** Bitdefender Endpoint Security Tools for Windows fungiert als auf den Endpunkten installierter Einspeisungssensor. Der Bitdefender-Agent verwendet fortschrittliche Algorithmen des maschinellen Lernens und des neuronalen Netzwerks, um verdächtige Inhalte zu erkennen und an Sandbox Analyzer zu übermitteln, einschließlich Objekte aus der zentralen Quarantäne.

- **Netzwerksensor.** Network Security Virtual Appliance (NSVA) ist eine virtuelle Appliance, die in derselben virtualisierten ESXi-Umgebung wie die Sandbox Analyzer-Instanz bereitgestellt werden kann. Der Netzwerksensor erfasst Inhalte aus Netzwerkdatenströmen und übermittelt diese an Sandbox Analyzer.
- **ICAP-Sensor.** Auf NAS-Geräten (Network Attached Storage) mit ICAP-Protokoll bereitgestellt, unterstützt Bitdefender Security Server die Übertragung von Inhalten an Sandbox Analyzer.

Zusätzlich zu diesen Sensoren unterstützt Sandbox Analyzer On-Premises auch die manuelle Übertragung und die Übertragung über die API. Weitere Einzelheiten entnehmen Sie dem Kapitel **Verwendung von Sandbox Analyzer** im GravityZone-Administratorhandbuch.

4. ERSTE SCHRITTE

GravityZone-Lösungen können über eine zentrale Verwaltungsplattform namens Control Center konfiguriert und verwaltet werden. Control Center hat eine Web-basierte Oberfläche, auf die Sie mit einem Benutzernamen und einem Passwort zugreifen können.

4.1. Verbinden mit dem Control Center

Der Zugriff auf die Control Center erfolgt über Benutzerkonten. Sie erhalten Ihre Anmeldeinformationen per E-Mail, sobald Ihr Konto angelegt wurde.

Vorbereitende Maßnahmen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Empfohlene Bildschirmauflösung: mindestens 1280 x 800



Warnung

Control Center funktioniert in der Kompatibilitätsansicht des Internet Explorer 9+ nicht bzw. wird nicht richtig angezeigt. Es ist, als würden Sie eine nicht unterstützte Browserversion benutzen.

So stellen Sie eine Verbindung zum Control Center her:

1. Geben Sie in die Adressleiste ihres Browsers IP-Adresse oder den DNS-Hostnamen der Control Center-Appliance ein (mit dem Präfix `https://`).
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
3. Geben Sie den 6-stelligen Code aus dem Google Authenticator, Microsoft Authenticator oder einer beliebigen anderen Zwei-Faktor-Authentifizierungs-App (sofern sie mit dem [Standard RFC6238](#) kompatibel ist. Weitere Informationen finden Sie unter „[Verwalten Ihres Kontos](#)“ (S. 26).
4. Klicken Sie auf **Anmelden**.

Bei der ersten Anmeldung müssen Sie den Bitdefender-Nutzungsbedingungen zustimmen. Mit einem Klick auf **Fortfahren** können Sie mit der Nutzung von GravityZone loslegen.

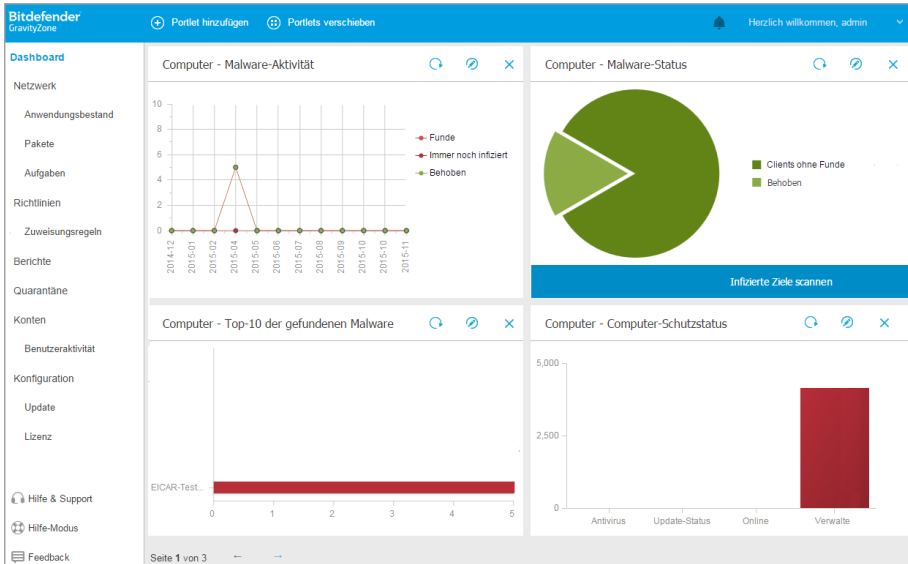


Beachten Sie

Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern. Sie müssen die E-Mail-Adresse Ihres Kontos angeben.

4.2. Control Center auf einen Blick


Control Center ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten. Verwenden Sie die Menüleiste auf der rechten Seite, um durch die Konsole zu navigieren. Welche Funktionen zur Verfügung stehen, hängt davon ab, welcher Benutzertyp auf die Konsole zugreift.



Das Dashboard

4.2.1. Übersicht über die Control Center

Benutzer mit der Unternehmensadministrator-Rolle haben volle Konfigurationsrechte für das Control Center und die Netzwerk Sicherheitsseinstellungen. Benutzer mit der Administrator-Rolle haben Zugriff auf Netzwerksicherheitsfunktion wie die Benutzerverwaltung.

Verwenden Sie die Schaltfläche  **Menü anzeigen** oben links, um in die Symbolansicht umzuschalten oder die Menüoptionen zu verbergen oder aufzuklappen. Klicken Sie auf die Schaltfläche, um die Optionen nacheinander durchzuschalten, oder doppelklicken Sie, um sie zu überspringen.

Abhängig von Ihrer Rolle stehen Ihnen die folgenden Menüpunkte zur Verfügung:

Dashboard

Übersichtliche Diagramme anzeigen, die wichtige Sicherheitsinformationen über Ihr Netzwerk enthalten.

Netzwerk

Schutz installieren, Richtlinien zur Verwaltung von Sicherheitseinstellungen anwenden, Aufgaben aus der Ferne ausführen und Schnellberichte erstellen.

Richtlinien

Sicherheitsrichtlinien erstellen und verwalten.

Berichte

Sicherheitsberichte über verwaltete Clients erhalten.

Quarantäne

Dateien in Quarantäne per Fernzugriff verwalten.

Konten

Zugriff zum Control Center anderer Mitarbeiter der Unternehmens verwalten.

In diesem Menü finden Sie auch die Seite **Benutzeraktivität**, über die Sie auf das Aktivitätsprotokoll zugreifen können.



Beachten Sie

Dieses Menü steht nur Benutzern zur Verfügung, die die Berechtigung **Benutzer verwalten** haben.

Konfiguration

Konfigurieren Sie Control Center-Einstellungen, wie z. B. Mailserver, Integration mit Active Directory oder Virtualisierungsumgebungen, Sicherheitszertifikate und Netzwerkinventareinstellungen, einschließlich geplanter Regeln für die automatische Bereinigung nicht verwendeter virtueller Maschinen.





Beachten Sie

Dieses Menü steht nur Benutzern zur Verfügung, die die Berechtigung **Lösung verwalten** haben.

Wenn Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole klicken, erhalten Sie die folgenden Optionen:

- **Mein Konto.** Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Zugangsdaten-Manager.** Klicken Sie auf diese Option, um die für Ferninstallationsaufgaben nötigen Authentifizierungsdaten hinzuzufügen und zu verwalten.
- **Hilfe & Support.** Klicken Sie auf diese Option, um Hilfe- und Support-Informationen zu erhalten.
- **Feedback.** Klicken Sie auf diese Option, um ein Formular zu öffnen, über das Sie uns Rückmeldung zu Ihren Erfahrungen mit GravityZone geben können.
- **Abmelden.** Klicken Sie auf diese Option, um sich bei Ihrem Konto abzumelden.

Rechts oben in der Konsole finden Sie außerdem:

- Das Symbol  **Hilfe-Modus**, über das Tooltips zu Elementen im Control Center angezeigt werden können. Dadurch erhalten Sie nützliche Informationen zu den Funktionen des Control Center.
- Das  **Benachrichtigungs-Symbol**, über das Sie einzelne Benachrichtigungen anzeigen und die Seite **Benachrichtigungen** öffnen können.

4.2.2. Tabellendaten

Tabellen kommen in der Konsole häufig zum Einsatz, um die Daten in einem übersichtlichen Format zu organisieren.

+ Hinzuf. ↓ Download − Löschen 🔄 Neu laden				
<input type="checkbox"/>	Berichtsname	Typ	Wiederholung	Bericht anzeigen
<input type="checkbox"/>	Malware-Aktivitätsbericht	Malware-Aktivität	Täglich	09 Okt 2015 - 02:00

Erste Seite -- Seite von 1 -- Letzte Seite 1 Objekt(e)

Die Berichteseite

Durch Tabellenseiten blättern

Tabellen mit mehr als 20 Einträgen haben mehr als eine Seite. Standardmäßig werden nur 20 Einträge pro Seite angezeigt. Verwenden Sie die

Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Sie können die Anzahl der Einträge, die pro Seite angezeigt werden, ändern, indem Sie eine andere Option aus dem Menü neben den Navigationsschaltflächen wählen.

Nach bestimmten Einträgen suchen

Über die Suchfelder unter den Spaltenüberschriften können Sie leicht bestimmte Einträge finden.

Geben Sie den Suchbegriff in das entsprechende Feld ein. Passende Suchtreffer werden bereits während der Eingabe in der Tabelle angezeigt. Um den Inhalt der Tabelle wieder herzustellen, löschen Sie einfach die Suchfelder.

Daten sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Mit einem erneuten Klick auf die Spaltenüberschrift kehren Sie die Sortierreihenfolge um.




Tabellendaten neu laden

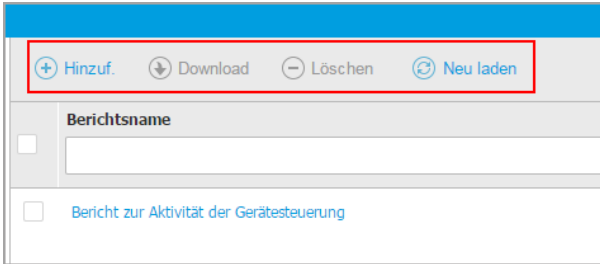
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf  **Neu laden**.

Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

4.2.3. Symbolleisten

Im Control Center können Sie über Symbolleisten bestimmte Operationen ausführen, die zu dem Bereich gehören, indem Sie sich gerade befinden. Jede Symbolleiste besteht aus mehreren Symbolen, die meistens am oberen Rand der Tabelle angezeigt werden. Über die Symbolleiste im Bereich **Berichte** können Sie zum Beispiel die folgenden Aktionen ausführen:

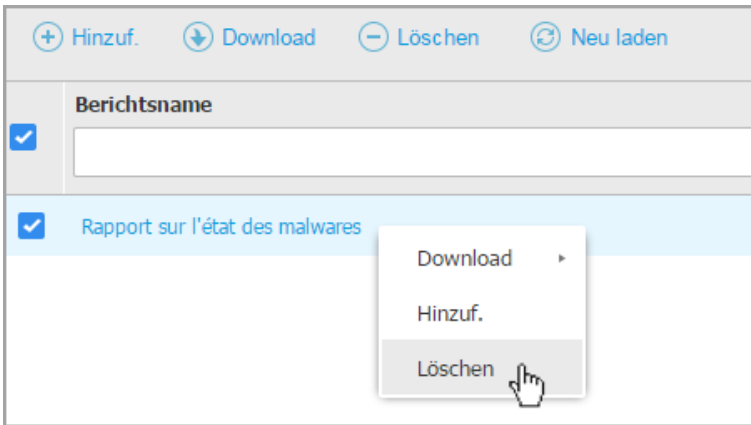
-  Neuen Bericht erstellen.
-  Einen geplanten Bericht herunterladen.
-  Einen geplanten Bericht löschen.



Die Berichteseite - Symbolleiste

4.2.4. Kontextmenü

Die Symbolleistenbefehle stehen auch über das Kontextmenü zur Verfügung. Klicken Sie mit der rechten Maustaste auf den Bereich des Control Centers, den Sie gerade benutzen, und wählen Sie den gewünschten Befehl aus der Liste.



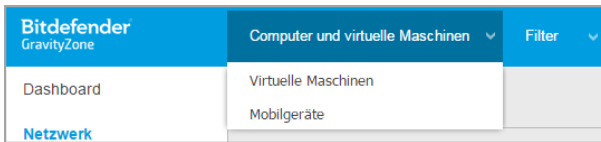
Die Berichteseite - Kontextmenü

4.2.5. Ansichtsauswahl

Wenn Sie mit verschiedenen Arten von Endpunkten arbeiten, finden Sie sie auf der Seite **Netzwerk** nach Typ sortiert auf verschiedene Netzwerkansichten verteilt:

- **Computer & virtuelle Maschinen:** zeigt Active-Directory-Gruppen und Computer sowie physische und virtuelle Arbeitsstationen außerhalb des Active Directory, die im Netzwerk gefunden wurden, an.
- **Virtuelle Maschinen:** zeigt die Infrastruktur der virtuellen Umgebung an, die mit dem Control Center integriert ist, sowie alle darin enthaltenen virtuellen Maschinen.
- **Mobilgeräte:** zeigt Benutzer und die ihnen zugewiesenen Geräte an.

Um die gewünschte Netzwerkansicht anzuzeigen, klicken Sie auf das Ansichtenmenü in der rechten oberen Ecke der Seite.



Die Ansichtsauswahl



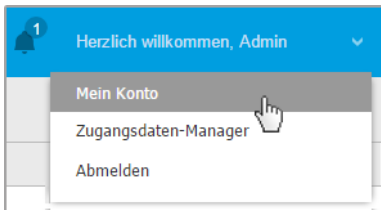
Beachten Sie

Es werden Ihnen nur diejenigen Endpunkte angezeigt, für die Ihnen der Administrator, der Ihren Benutzer zum Control Center hinzugefügt hat, Rechte erteilt hat.

4.3. Verwalten Ihres Kontos

So überprüfen oder ändern Sie Ihre Kontodetails und -Einstellungen:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.



Das Benutzerkontomenü

2. Korrigieren oder aktualisieren Sie Ihre Kontoinformationen unter **Kontodetails**. Wenn Sie ein Active-Directory-Benutzerkonto verwenden, können Sie die Kontodetails nicht ändern.
 - **Nutzername**. Der Benutzername ist der eindeutige Identifikator eines Benutzerkontos und kann daher nicht geändert werden.
 - **Vollständiger Name**. Geben Sie Ihren vollen Namen ein.
 - **E-Mail**. Dies ist Ihre E-Mail-Adresse für die Anmeldung und den Kontakt. An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt. Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
 - Über den Link **Passwort ändern** können Sie Ihr Anmeldepasswort ändern.
3. Konfigurieren Sie die Kontoeinstellungen unter **Einstellungen** nach Ihren Wünschen.
 - **Zeitzone**. Wählen Sie im Menü die Zeitzone für Ihr Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
 - **Sprache**. Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
 - **Zeitüberschreitung der Sitzung**. Legen Sie den Inaktivitätszeitraum fest, nach dem Ihre Sitzung abläuft.
4. Konfigurieren Sie unter **Sicherheit des Anmeldevorgangs** die Zwei-Faktor-Authentifizierung und überprüfen Sie den Status der Richtlinien, die zur Absicherung Ihres GravityZone-Kontos verfügbar sind. Unternehmensweit festgelegte Richtlinien sind schreibgeschützt.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

- a. **Zwei-Faktor-Authentifizierung**. Die Zwei-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsschicht für Ihr GravityZone-Konto, da sie erfordert, dass Sie bei der Anmeldung an Ihrem Konto außer den Zugangsdaten für das Control Center noch einen Authentifizierungscode eingeben.

Wenn Sie sich zum ersten Mal bei Ihrem GravityZone-Benutzerkonto anmelden, werden Sie aufgefordert, den Google Authenticator, Microsoft Authenticator oder eine beliebige andere, mit dem [RFC6238-Standard](#) kompatible Anwendung zur Zwei-Faktor-Authentifizierung mit TOTP (Time-Based One-Time Password Algorithm) auf ein Mobilgerät herunterzuladen und zu installieren, mit Ihrem GravityZone-Benutzerkonto zu verknüpfen und dann bei jeder Control Center-Anmeldung zu verwenden. Google Authenticator erzeugt alle 30 Sekunden einen neuen sechsstelligen Code. Um sich am Control Center anzumelden, müssen Sie nach der Eingabe

Ihrer Zugangsdaten den sechsstelligen Code aus Google Authenticator eingeben.



Beachten Sie

Sie können diesen Prozess bis zu dreimal überspringen, danach können Sie sich nicht mehr ohne Zwei-Faktor-Authentifizierung anmelden.

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

- i. Klicken Sie unter der Meldung **Zwei-Faktor-Authentifizierung** auf **Aktivieren**.
- ii. Klicken Sie im Dialogfeld auf den entsprechenden Link, um Google Authenticator herunterzuladen und auf Ihrem Mobilgerät zu installieren.
- iii. Öffnen Sie Google Authenticator auf Ihrem Mobilgerät.
- iv. Scannen Sie im Bildschirm **Konto hinzufügen** den QR-Code, um die App mit Ihrem GravityZone-Konto zu verknüpfen.

Sie können auch den geheimen Schlüssel manuell eingeben.

Dieser Vorgang muss nur einmal durchgeführt werden, damit die Funktion in GravityZone aktiviert wird.



Wichtig

Vergessen Sie nicht, den geheimen Schlüssel an einem sicheren Ort aufzubewahren. Klicken Sie auf **Backup drucken**, um eine PDF-Datei mit dem QR-Code und dem geheimen Schlüssel anzulegen. Wenn Sie das Mobilgerät, das Sie zur Aktivierung der Zwei-Faktor-Authentifizierung benutzt haben, nicht mehr haben (verloren, kaputt, ...), müssen Sie Google Authenticator auf einem neuen Gerät installieren und dort den geheimen Schlüssel eingeben, um das neue Gerät mit Ihrem GravityZone-Konto zu verknüpfen.

- v. Geben Sie den sechsstelligen Code in das Feld **Google-Authenticator-Code** ein.
- vi. Klicken Sie auf **Aktivieren**, um die Funktion zu aktivieren.



Beachten Sie

Ihr Unternehmensadministrator kann die Zwei-Faktor-Authentifizierung für alle GravityZone-Benutzerkonten zwingend erforderlich machen. Ist dies der Fall, werden Sie bei der Anmeldung aufgefordert, Ihre 2FA zu konfigurieren.

Sie können die Zwei-Faktor-Authentifizierung (2FA) für Ihr Benutzerkonto zudem nicht deaktivieren, solange diese Funktion durch Ihren Unternehmensadministrator zwingend vorgeschrieben ist.

Bitte beachten Sie, dass dieser geheime Schlüssel seine Gültigkeit verliert, wenn die aktuell konfigurierte 2FA für Ihr Benutzerkonto deaktiviert wird,

- b. **Passwortablaufrichtlinie.** Durch regelmäßige Änderung Ihres Passworts erhalten Sie zusätzlichen Schutz vor nicht autorisierter Verwendung von Passwörtern oder begrenzen die Dauer von nicht autorisierter Verwendung. Wenn diese Richtlinie aktiviert ist, müssen Sie Ihr GravityZone-Passwort spätestens alle 90 Tage ändern.
- c. **Kontosperrungsrichtlinie.** Diese Richtlinie verhindert den Zugriff auf Ihr Konto nach fünf aufeinander folgenden fehlgeschlagenen Anmeldeversuchen. Diese Maßnahme dient dem Schutz vor Brute-Force-Angriffen.

Um Ihr Konto zu entsperren, müssen Sie Ihr Passwort auf der Anmeldeseite zurücksetzen oder einen anderen GravityZone-Administrator kontaktieren.

5. Klicken Sie **Speichern**, um die Änderungen zu speichern.



Beachten Sie

Sie können Ihr eigenes Konto nicht löschen.

4.4. Ändere Login Passwort

Nachdem Ihr Konto angelegt wurde, erhalten Sie eine E-Mail mit den Anmeldedaten. Sofern Sie keine Active-Directory-Zugangsdaten für den Zugriff auf Control Center verwenden, sollten Sie wie folgt vorgehen:

- Ändern Sie das Standardpasswort nach dem ersten Aufrufen von Control Center.
- Ändern Sie Ihr Kennwort regelmäßig.

Um das Anmeldepasswort zu ändern:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.
2. Klicken Sie unter **Kontodetails** auf **Passwort ändern**.
3. Geben Sie Ihr aktuelles Passwort und das neue Passwort in die entsprechenden Felder ein.
4. Klicken Sie **Speichern**, um die Änderungen zu speichern.

5. BENUTZERKONTEN

Sie können das erste GravityZone-Benutzerkonto während der Ersteinrichtung des Control Center nach der Installation der GravityZone-Appliance erstellen. Das erste Benutzerkonto für Control Center hat die Unternehmensadministrator-Rolle mit vollen Rechten über die Konfiguration des Control Center und die Netzwerkverwaltung. Von diesem Konto aus können Sie alle anderen Benutzerkonten erstellen, die Sie für die Verwaltung Ihres Unternehmensnetzwerks benötigen.

Mit den folgenden Punkten zu den GravityZone-Benutzerkonten sollten Sie vertraut sein:

- Um auch anderen Mitarbeitern des Unternehmens den Zugriff auf das Control Center zu erlauben, können Sie einzelne Benutzerkonten erstellen oder per Active Directory-Integrationen oder Zugriffsregeln den dynamischen Zugriff für mehrere Benutzerkonten erlauben. Sie können Benutzerkonten verschiedene Rollen mit unterschiedlichen Zugriffsrechten zuweisen.
- Für jedes Benutzerkonto können Sie den Zugriff auf GravityZone-Funktionen oder bestimmte Teile des Netzwerks, zu dem es gehört, festlegen.
- Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.

Benutzername	E-Mail	Rolle	Dienste
<input type="checkbox"/> reporter	office@comp.com	Berichterstatter	Computer, Virtuelle Maschinen
<input type="checkbox"/> admin	admin@office.com	Unternehmensadministrator	Computer, Virtuelle Maschinen, Mobilgeräte

Die Kontenübersicht

Bestehende Konten werden in der Tabelle angezeigt. Sie können das Folgende für jedes Benutzerkonto einsehen:

- Der Benutzername des Kontos (wird zur Anmeldung an der Control Center verwendet).
- E-Mail-Adresse des Kontos (wird als Kontaktadresse verwendet). An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt. Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
- Benutzerrolle (Unternehmensadministrator / Netzwerkadministrator / Sicherheitsanalyst/ benutzerdefiniert)
- GravityZone-Sicherheitsdienste, die der Benutzer verwalten darf (Computer, virtuelle Maschinen, Mobilgeräte).
- Der Status der Zwei-Faktor-Authentifizierung (2FA). Hier können Sie überprüfen, ob der Benutzer die Zwei-Faktor-Authentifizierung aktiviert hat.
- Zugriffsregel-Status; zeigt an, ob ein Benutzerkonto über eine Zugriffsberechtigungsregel erstellt wurde. Für manuell erstellte Benutzerkonten wird **N/A** angezeigt.

5.1. Benutzerrollen

Eine Benutzerrolle umfasst eine bestimmte Kombination aus Benutzerrechten. Wenn Sie ein Benutzerkonto anlegen, können Sie eine der vordefinierten Rollen wählen oder eine benutzerdefinierte Rolle erstellen, indem Sie nur die gewünschten Benutzerrechte auswählen.



Beachten Sie

Sie können anderen Benutzerkonten nur die Rechte zuweisen, über die Sie selbst verfügen.

Die folgenden Benutzerrollen sind verfügbar:

1. **Unternehmensadministrator** - In der Regel wird für jedes Unternehmen ein einziges Benutzerkonto mit der Unternehmensadministrator-Rolle angelegt, das vollen Zugriff auf alle Verwaltungsfunktionen der GravityZone-Lösungen ermöglicht. Ein Unternehmensadministrator kann die Control Center-Einstellungen konfigurieren, Lizenzschlüssel für die Sicherheitsdienste verwalten und Benutzerkonten verwalten. Er verfügt zudem über Administratorrechte für die Sicherheitseinstellungen im Unternehmensnetzwerks. Unternehmensadministratoren können ihre Aufgaben

mit untergeordneten Administrator- und Sicherheitsanalytikerkonten teilen oder diese an sie delegieren.

2. **Netzwerkadministrator** - Für ein Unternehmen können mehrere Benutzerkonten mit der Netzwerkadministrator-Rolle angelegt werden. Diese verfügen über Administratorrechte für alle Sicherheitsagenten im Unternehmen bzw. für eine festgelegte Gruppe von Endpunkten; das schließt die Benutzerverwaltung ein. Netzwerkadministratoren sind zuständig für die aktive Verwaltung der Sicherheitseinstellungen im Netzwerk.
3. **Sicherheitsanalyst** - Sicherheitsanalytikerkonten haben nur Lesezugriff. Über sie besteht nur Zugriff auf sicherheitsrelevante Daten, Berichte und Protokolle. Diese Benutzerkonten sind für Mitarbeiter gedacht, die mit der Überwachung der Unternehmenssicherheit betraut sind, und solche, die über die Sicherheitslage auf dem Laufenden gehalten werden müssen.
4. **Benutzerdefiniert** - Vordefinierte Benutzerrollen beinhalten eine bestimmte Kombination aus Berechtigungen. Sollte eine vordefinierte Benutzerrolle Ihren Anforderungen nicht entsprechen, können Sie ein benutzerdefiniertes Konto mit genau den Rechten anlegen, die Sie benötigen.

Die nachfolgende Tabelle gibt einen Überblick über die Zusammenhänge zwischen den verschiedenen Rollen und ihren Berechtigungen. Detaillierte Informationen finden Sie unter „Benutzerrechte“ (S. 33).

Rolle des Kontos	Zugelassene untergeordnete Konten	Benutzerrechte
Unternehmensadministrator	Unternehmensadministratoren, Netzwerkadministratoren, Sicherheitsanalysten	Lösung verwalten Eigenes Unternehmen verwalten Benutzer verwalten Netzwerke verwalten Daten anzeigen und analysieren
Netzwerkadministrator	Netzwerkadministratoren, Sicherheitsanalysten	Benutzer verwalten Netzwerke verwalten Daten anzeigen und analysieren
Sicherheitsanalysten	-	Daten anzeigen und analysieren

5.2. Benutzerrechte

Sie können den GravityZone-Benutzerkonten die folgenden Benutzerrechte zuweisen:

- **Lösung verwalten.** Berechtigt zur Konfiguration von Einstellungen für Control Center (Mail-Server und Proxy-Einstellungen, Integration mit Active Directory und Virtualisierungsplattformen, Sicherheitszertifikate und GravityZone-Updates). Dieses Recht haben nur Unternehmensadministratoren.
- **Benutzer verwalten.** Benutzerkonten erstellen, bearbeiten oder löschen.
- **Eigenes Unternehmen verwalten.** Benutzer können ihren eigenen GravityZone-Lizenzschlüssel verwalten und die Einstellungen für ihr Unternehmensprofil bearbeiten. Dieses Recht haben nur Unternehmensadministratoren.
- **Netzwerke verwalten.** Gewährt Administrationsrechte über die Netzwerksicherheitseinstellungen (Netzwerkinventar, Richtlinien, Aufgaben, Installationspakete, Quarantäne). Dieses Recht haben nur Netzwerkadministratoren.
- **Daten anzeigen und analysieren.** Sicherheitsrelevante Ereignisse und Protokolle anzeigen, Berichte und das Dashboard verwalten.

5.3. Benutzerkonten verwalten

Verwenden Sie die folgenden Methoden, um Benutzerkonten zu erstellen, zu bearbeiten, zu löschen und zu konfigurieren:

- **Einzelverwaltung von Benutzerkonten.** Verwenden Sie diese Methode, um lokale Benutzerkonten oder Active Directory-Konten hinzuzufügen. Weitere Informationen zur Einrichtung der Active Directory-Integration finden Sie in der GravityZone-Installationsanleitung.

Bevor Sie ein Benutzerkonto anlegen, sollten Sie sicherstellen, dass Sie die benötigte E-Mail-Adresse zur Hand haben. Dem Benutzer werden die GravityZone-Zugangsdaten an die angegebene E-Mail-Adresse gesendet.

- **Verwaltung mehrerer Benutzerkonten.** Verwenden Sie diese Methode, um den dynamischen Zugriff über Zugriffsberechtigungsregeln zu ermöglichen. Diese Methode erfordert eine Active Directory-Domänenintegration. Weitere Informationen zur Active Directory-Integration finden Sie in der GravityZone-Installationsanleitung.

5.3.1. Einzelverwaltung von Benutzerkonten

Im Control Center können Sie Benutzerkonten einzeln erstellen, bearbeiten und löschen.

Abhängigkeiten

- Lokal erstellte Benutzerkonten können Benutzerkonten, die über die Active Directory-Integration erstellt wurden, unabhängig von ihrer Rolle löschen.
- Lokal erstellte Benutzerkonten können vergleichbare Benutzerkonten unabhängig von ihrer Rolle nicht löschen.

Benutzerkonten einzeln erstellen

So fügen Sie im Control Center ein Benutzerkonto hinzu:

1. Rufen Sie die Seite **Konten** auf.
2. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
3. Nehmen Sie im Abschnitt **Details** die folgenden Konfigurationen vor:
 - Konfigurieren Sie für Active Directory-Benutzerkonten die folgenden Details:

Benutzername für Active Directory (AD)-Benutzerkonten. Wählen Sie ein Benutzerkonto aus der Dropdown-Liste und fahren Sie mit Schritt 4 fort.

Sie können AD-Benutzerkonten nur dann hinzufügen, wenn die Integration konfiguriert ist. Beim Hinzufügen eines AD-Benutzerkontos werden die Benutzerdaten aus der zugehörigen Domäne importiert. Der Benutzer meldet sich mit seinem AD-Benutzernamen und dem Passwort beim Control Center an.



Beachten Sie

- Um sicherzustellen, dass die neuesten Änderungen in Active Directory auch in die Control Center importiert werden, klicken Sie auf die Schaltfläche **Synchronisieren**.
- Benutzer mit der Berechtigung **Lösung verwalten** können das Active-Directory-Synchronisierungsintervall über die Optionen im Reiter **Konfiguration > Active Directory** konfigurieren. Weitere Details erfahren Sie in den Kapiteln **Schutz installieren > GravityZone-Installation** sowie

Einrichtung > Control Center-Einstellungen konfigurieren der GravityZone-Installationsanleitung.

- Konfigurieren Sie für lokale Benutzerkonten die folgenden Details:
 - **Benutzername** für das lokale Konto. Deaktivieren Sie **Import aus Active Directory** und geben Sie einen Benutzernamen ein.
 - **E-Mail**. Geben Sie die E-Mail-Adresse des Benutzers ein.

Die E-Mail-Adresse darf nur einmal vergeben werden. Sie können keine weiteren Benutzerkonten mit der gleichen E-Mail-Adresse anlegen. GravityZone verwendet diese E-Mail-Adresse zur Übermittlung von Benachrichtigungen.
 - **Vollständiger Name**. Geben Sie den vollständigen Namen des Benutzers ein.
 - **Passwort**. Geben Sie ein Passwort ein, mit dem sich der Benutzer anmelden kann.

Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten.
 - **Passwort bestätigen**. Bestätigen Sie das Passwort.
- 4. Konfigurieren Sie im Bereich **Einstellungen und Rechte** die folgenden Einstellungen:
 - **Zeitzone**. Wählen Sie im Menü die Zeitzone für das Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
 - **Sprache**. Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
 - **Rolle**. Wählen Sie die Rolle des Benutzers aus. Weitere Details zu Benutzerrollen finden Sie unter „[Benutzerrollen](#)“ (S. 31).
 - **Rechte**. Jede vordefinierte Benutzerrolle verfügt über einen bestimmten Satz von Rechten. Sie können dabei aber genau die Rechte auswählen, die Sie benötigen. Die Benutzerrolle wechselt dann zu **Benutzerdefiniert**. Weitere Informationen zu den Benutzerrechten finden Sie unter „[Benutzerrechte](#)“ (S. 33).
 - **Ziele wählen**. Wählen Sie für jeden verfügbaren Sicherheitsdienst die Netzwerkgruppen, auf die der Benutzer Zugriff haben soll. Sie können den

Zugriff eines Benutzers auf bestimmte GravityZone-Sicherheitsdienste oder auf bestimmte Bereiche des Netzwerks beschränken.



Beachten Sie

Die Optionen für die Zielauswahl werden nicht für Benutzer mit dem Recht zur Lösungsverwaltung angezeigt. Diese haben standardmäßig Rechte für das gesamte Netzwerk und die Sicherheitsdienste.



Wichtig

Vergessen Sie nicht, jedes Mal, wenn Sie Änderungen an Ihrer Netzwerkstruktur vornehmen oder eine neue Integration mit einem anderen vCenter Server- oder XenServer-System einrichten, die Zugriffsrechte bestehender Benutzer zu überprüfen und gegebenenfalls anzupassen.

5. Klicken Sie auf **Speichern**, um den Benutzer hinzuzufügen. Das neue Konto erscheint in der Liste der Benutzerkonten.

Control Center sendet dem Benutzer automatisch eine E-Mail mit den Zugangsdaten, sofern die Mail-Server-Einstellungen korrekt konfiguriert wurden. Weitere Details zur Mail-Server-Konfiguration erfahren Sie im Kapitel **Schutz installieren > GravityZone-Installation und Einrichtung > Control Center-Einstellungen konfigurieren** der GravityZone-Installationsanleitung.

Benutzerkonten einzeln bearbeiten

So fügen Sie im Control Center ein Benutzerkonto hinzu

1. Melden Sie sich im Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Ändern Sie die Details und Einstellungen für das Benutzerkonto nach Bedarf.
5. Klicken Sie **Speichern**, um die Änderungen zu speichern.




Beachten Sie

Alle Konten mit der Berechtigung **Benutzer verwalten** können andere Konten erstellen, bearbeiten und löschen. Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.

Benutzerkonten einzeln löschen

So löschen Sie ein Benutzerkonto im Control Center:

1. Melden Sie sich im Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Wählen Sie das Benutzerkonto aus der Liste aus.
4. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle.
Klicken Sie zur Bestätigung auf **Ja**.

5.3.2. Verwaltung mehrerer Benutzerkonten

Erstellen Sie Zugriffsregeln, um dem GravityZone Control Center auf der Basis von Sicherheitsgruppen Zugriff auf Active-Directory-Benutzer zu gewähren.

Vorbereitende Maßnahmen

Zur Verwaltung mehrerer Benutzerkonten benötigen Sie eine Active Directory-Domänenintegration mit GravityZone. Informationen zur Integration und Synchronisierung einer Active Directory-Domäne finden Sie im Kapitel **Active Directory** im GravityZone-Installationshandbuch.

Abhängigkeiten

Zugriffsberechtigungsregeln sind an die Sicherheitsgruppen von Active Directory (AD) und die zugehörigen Benutzerkonten gebunden. Jede Änderung an den Active Directory-Domänen kann sich auf die zugehörigen Zugriffsberechtigungsregeln auswirken. Wichtige Informationen zu den Beziehungen zwischen Regeln, Benutzern und Active Directory-Domänen:

- Über eine Zugriffsberechtigungsregel wird nur dann ein Benutzerkonto erstellt, wenn die E-Mail nicht bereits einem bestehenden Konto zugewiesen ist.
- Bei doppelt vorkommenden E-Mail-Adressen innerhalb einer Sicherheitsgruppe erstellt die Zugriffsberechtigungsregel ein GravityZone-Benutzerkonto nur für das erste Active Directory-Benutzerkonto, das sich am Control Center anmeldet.

Eine Sicherheitsgruppe enthält beispielsweise eine doppelt vorkommende E-Mail-Adresse für verschiedene Benutzer, die dann versuchen, sich mit ihren Active Directory-Anmeldeinformationen beim Control Center anzumelden. Wenn dieser Active Directory-Domäne eine Zugriffsberechtigungsregel zugeordnet

ist, wird nur für den ersten Benutzer ein Benutzerkonto erstellt, der sich mit der doppelt vorkommenden E-Mail-Adresse am Control Center angemeldet hat.

- Über Zugriffsberechtigungsregeln erstellte Benutzerkonten werden inaktiv, wenn sie aus ihrer AD-Sicherheitsgruppe entfernt werden. Diese Benutzer können aktiv werden, wenn sie einer neuen Zugriffsregel zugewiesen werden.
- Zugriffsregeln werden schreibgeschützt, sobald die entsprechende Active Directory-Domäne nicht mehr in GravityZone integriert ist. Zu diesen Regeln gehörige Benutzer werden inaktiv.
- Über Zugriffsregeln erstellte Benutzerkonten können lokal erstellte Benutzer nicht löschen.
- Über Zugriffsregeln erstellte Benutzerkonten können vergleichbare Benutzerkonten mit der Rolle Unternehmensadministrator nicht löschen.

Erstellen mehrerer Benutzerkonten

Erstellen Sie Zugriffsberechtigungsregeln, um mehrere Benutzerkonten hinzuzufügen. Die Zugriffsberechtigungsregeln sind den Active Directory-Sicherheitsgruppen zugeordnet.

So fügen Sie eine Zugriffsberechtigungsregel hinzu:

1. Gehen Sie zu **Konfiguration > Active Directory > Zugriffsberechtigungen**.
2. Wenn Sie mehrere Integrationen haben, wählen Sie links oben an der Tabelle eine Domain.
3. Klicken Sie links auf **+ Hinzufügen**.
4. Konfigurieren Sie die folgenden Zugriffsberechtigungeinstellungen:
 - **Priorität.** Regeln sind nach Priorität sortiert. Die kleinste Zahl bekommt die höchste Priorität.
 - **Name.** Name der Zugriffsregel.
 - **Domain.** Domain, von der Sicherheitsgruppen hinzugefügt werden sollen.
 - **Sicherheitsgruppen.** Die Sicherheitsgruppen, in denen die zukünftigen GravityZone-Benutzer enthalten sind. Sie können die Vervollständigungsbox benutzen. Sicherheitsgruppen, die Sie dieser Liste hinzufügen, können nicht mehr geändert, erweitert oder gelöscht werden, nachdem Sie die Zugriffsregel gespeichert haben.
 - **Zeitzone.** Zeitzone des Benutzers.

- **Sprache.** Sprache der Benutzeroberfläche.
- **Rolle.** Vordefinierte Benutzerrollen. Weitere Einzelheiten entnehmen Sie dem Kapitel **Benutzerkonten** des GravityZone-Administratorhandbuchs.

**Beachten Sie**

Sie können anderen Benutzern Rechte erteilen und entziehen, sofern diese Benutzer nicht über mehr Rechte verfügen als Sie.

- **Rechte.** Jede vordefinierte Benutzerrolle verfügt über einen bestimmten Satz von Rechten. Weitere Einzelheiten entnehmen Sie dem Kapitel **Benutzerrechte** des GravityZone-Administratorhandbuchs.
- **Ziele wählen** Wählen Sie für jeden verfügbaren Sicherheitsdienst die Netzwerkgruppen, auf die der Benutzer Zugriff haben soll. Sie können den Zugriff eines Benutzers auf bestimmte GravityZone-Sicherheitsdienste oder auf bestimmte Bereiche des Netzwerks beschränken.

**Beachten Sie**

Die Optionen für die Zielauswahl werden nicht für Benutzer mit dem Recht zur Lösungsverwaltung angezeigt. Diese haben standardmäßig Rechte für das gesamte Netzwerk und die Sicherheitsdienste.

5. Klicken Sie auf **Speichern**.

Die Zugriffsregel wird gespeichert, wenn es dadurch zu keinerlei Auswirkungen auf Benutzer kommt. Andernfalls werden Sie aufgefordert, einzelne Benutzer auszuschließen. Wenn Sie zum Beispiel eine Regel mit einer höheren Priorität hinzufügen, werden die betroffenen Benutzer, die anderen Regeln zugewiesen sind, an die neue Regel gebunden.

6. Wählen Sie bei Bedarf die Benutzer, die Sie ausschließen möchten. Weitere Details hierzu finden Sie unter [Benutzerkontoausschlüsse](#).
7. Klicken Sie auf **Bestätigen**. Die Regel wird auf der Seite **Zugriffsberechtigungen** angezeigt.

Benutzer in den Sicherheitsgruppen, die in den Zugriffsregeln definiert wurden, können jetzt mithilfe ihrer Domain-Zugangsdaten auf das GravityZone Control Center zugreifen. Wenn sich der Benutzer zum ersten Mal am Control Center anmeldet, wird auf der Grundlage der Active-Directory-E-Mail-Adresse und des zugehörigen Passworts automatisch ein neues Benutzerkonto erstellt.

Für Benutzerkonten, die über eine Zugriffsregel erstellt wurden, wird auf der Seite **Konten** in der Spalte **Zugriffsregel** der Name der Zugriffsregel angezeigt.

Bearbeiten mehrerer Benutzerkonten

So bearbeiten Sie eine Zugriffsberechtigungsregel:

1. Gehen Sie zu **Konfiguration > Active Directory > Zugriffsberechtigungen**.
2. Klicken Sie auf den Namen Ihrer Zugriffsregel, um das Konfigurationsfenster zu öffnen.
3. Bearbeiten Sie die Einstellungen für die Zugriffsberechtigungen. Weitere Informationen finden Sie unter [Zugriffsberechtigungen hinzufügen](#).
4. Klicken Sie auf **Speichern**. Die Regel wird gespeichert, wenn sie keine Auswirkungen auf Benutzer hat. Andernfalls werden Sie aufgefordert, einzelne Benutzerkonten auszuschließen. Wenn Sie zum Beispiel die Priorität einer Regel ändern, können betroffene Benutzer zu einer anderen Regel wechseln.
5. Wählen Sie bei Bedarf die Benutzer, die Sie ausschließen möchten. Weitere Details hierzu finden Sie unter [Benutzerkontoausschlüsse](#).
6. Klicken Sie auf **Bestätigen**.



Beachten Sie

Sie können die Verknüpfung von Benutzerkonten, die über eine Zugriffsregel erstellt wurden, entfernen, indem Sie deren Rechte im Control Center ändern. Das Benutzerkonto kann nicht wieder mit der Zugriffsregel verknüpft werden.

Löschen mehrerer Benutzerkonten

So löschen Sie eine Zugriffsregel:

1. Gehen Sie zu **Konfiguration > Active Directory > Zugriffsberechtigungen**.
2. Wählen Sie die Zugriffsregel, die Sie löschen möchten, und klicken Sie auf **Löschen**. Sie werden in einem Fenster aufgefordert, die Aktion zu bestätigen. Wenn es Auswirkungen auf den Benutzer gibt, werden Sie aufgefordert, Benutzerkontoausschlüsse anzugeben. Sie können zum Beispiel Ausschlüsse für Benutzer definieren, die von der Löschung einer Regel betroffen wären.
3. Wählen Sie bei Bedarf die Benutzer, die Sie ausschließen möchten. Weitere Details hierzu finden Sie unter [Benutzerausschlüsse](#).
4. Klicken Sie auf **Bestätigen**.

Wenn Sie eine Regel löschen, wird den entsprechenden Benutzerkonten der Zugriff wieder entzogen. Alle Benutzer, die über diese Regel erstellt wurden, werden entfernt, sofern Ihnen nicht durch andere Regeln Zugriff gewährt wird.

Benutzerkontoausschlüsse

Wenn Sie Zugriffsberechtigungsregeln hinzufügen, bearbeiten oder löschen und sich dieser Vorgang auf einzelne Benutzer auswirkt, können Sie Ausschlüsse für diese Benutzerkonten definieren. Sie können sich Details und Gründe zu diesen Auswirkungen anzeigen lassen.

So definieren Sie Benutzerausschlüsse:

1. Wählen Sie die Benutzer, die Sie ausschließen möchten. Oder markieren Sie das Kästchen am oberen Rand der Tabelle, um alle Benutzer hinzuzufügen.
2. Klicken Sie auf das **X** eines Benutzernamensfelds, um diesen Benutzer aus der Liste zu entfernen.

5.4. Anmeldepasswörter zurücksetzen

Kontoinhaber, die ihr Passwort vergessen haben, können es über den Link für die Passwortwiederherstellung auf der Anmeldeseite zurücksetzen. Sie können ein vergessenes Anmeldepasswort auch zurücksetzen, indem Sie das entsprechende Konto über die Konsole bearbeiten.

Um das Anmeldepasswort für einen Benutzer zurückzusetzen:

1. Melden Sie sich im Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Geben Sie in die entsprechenden Felder ein neues Passwort ein (unter **Details**).
5. Klicken Sie **Speichern**, um die Änderungen zu speichern. Der Kontoeigentümer erhält dann eine E-Mail mit dem neuen Passwort.

5.5. Zwei-Faktor-Authentifizierung verwalten

Nach einem Klick auf das Benutzerkonto können Sie den 2FA-Status (aktiviert oder deaktiviert) im Bereich **Zwei-Faktor-Authentifizierung** einsehen. Die folgenden Aktionen sind möglich:

- **Die Zwei-Faktor-Authentifizierung für den Benutzer zurücksetzen oder deaktivieren.** Wenn ein Benutzer, bei dem 2FA aktiviert wurde, ein neues Mobilgerät erhält oder die Daten auf dem Gerät löscht und den geheimen Schlüssel verloren hat:
 1. Geben Sie Ihr GravityZone-Passwort in das entsprechende Feld ein.
 2. Klicken Sie auf **Zurücksetzen** (wenn 2FA erzwungen ist) oder **Deaktivieren** (wenn 2FA nicht erzwungen ist).
 3. Eine Bestätigungsmeldung informiert Sie darüber, dass die Zwei-Faktor-Authentifizierung für den aktuellen Benutzer zurückgesetzt / deaktiviert wurde.

Nach dem Zurücksetzen der 2FA für Benutzerkonten, bei denen die Funktion erzwungen wird, wird der Benutzer bei der Anmeldung in einem Konfigurationsfenster dazu aufgefordert, die Zwei-Faktor-Authentifizierung mit einem neuen geheimen Schlüssel erneut zu konfigurieren.
- Falls bei dem Benutzer die 2FA deaktiviert ist und Sie sie aktivieren möchten, müssen Sie den Benutzer darum bitten, diese Funktion über seine Benutzerkontoeinstellungen zu aktivieren.



Beachten Sie

Falls Sie über ein Unternehmensadministrator-Benutzerkonto verfügen, können Sie die Zwei-Faktor-Authentifizierung für alle GravityZone-Benutzerkonten zwingend erforderlich machen. Weitere Informationen finden Sie in der Installationsanleitung in den Abschnitten **Schutz installieren > GravityZone: Installation und Einrichtung > Control Center-Einstellungen konfigurieren**.



Wichtig

Die gewählte Authentifizierungsanwendung (Google Authenticator, Microsoft Authenticator oder eine beliebige mit dem [RFC6238-Standard](#) kompatible Anwendung zur Zwei-Faktor-Authentifizierung mit TOTP (Time-Based One-Time Password Algorithm) kombiniert den geheimen Schlüssel mit dem aktuellen Zeitstempel des Mobilgeräts, um den sechsstelligen Code zu generieren. Bitte beachten Sie, dass die Zeitstempel auf dem Mobilgerät und der GravityZone-Appliance übereinstimmen müssen, damit der sechsstellige Code gültig ist. Um Probleme bei der Synchronisation von Zeitstempeln zu vermeiden, empfehlen wir die Aktivierung der automatischen Datums- und Zeiteinstellung auf dem Mobilgerät.

Es ist auch möglich, 2FA-Änderungen im Zusammenhang mit den Benutzerkonten nachzuverfolgen, indem Sie die Seite [Konten > Benutzeraktivität](#) aufrufen und die folgenden Filter auf die Aktivitätsprotokolle anwenden:

- Bereich > Konten / Unternehmen
- Aktion > Änderung

Weitere Informationen zur Aktivierung von 2FA finden Sie unter „[Verwalten Ihres Kontos](#)“ (S. 26)

6. NETZWERKOBJEKTE VERWALTEN

Auf der Seite **Netzwerk** stehen verschiedene Funktionen zur Verwaltung der im Control Center verfügbaren Netzwerkobjekte (Computer, virtuelle Maschinen und Mobilgeräte) zur Verfügung. Der Bereich **Netzwerk** besteht aus zwei Fenstern, in denen der Status der Netzwerkobjekte in Echtzeit angezeigt wird:

Name	Betriebssystem	IP	Zuletzt	Bezeichnung
WINDOWS701	Windows	192.168.0.17	N/A	N/A
WIN_2K12_X64_EN	Windows Server 20...	10.10.123.210	Online	N/A
WIN_8_X86_ENGLI	Windows	10.10.112.59	N/A	N/A
WKS-W786	Windows	10.10.15.66	N/A	N/A
WORK-PC	Windows 7 Ultimate	172.20.54.88	13 Mar 2015, ...	N/A
X110DEMO	Windows Server 20...	10.10.240.201	Online	N/A
XIN732	Windows Server 20...	192.168.50.21	Online	N/A
XMBX002	Windows Server 20...	192.168.50.20	Online	N/A

Die Netzwerk-Übersicht

1. Im linken Fenster wird die Netzwerk-Baumansicht angezeigt. Je nach ausgewählter Netzwerkansicht wird hier auch die mit dem Control Center integrierte Netzwerkstruktur wie Active Directory, vCenter Server oder XenServer angezeigt.

Alle in Ihrem Netzwerk gefundenen Computer und virtuellen Maschinen, die zu keiner integrierten Infrastruktur gehören, werden unter **Benutzerdefinierte Gruppen** angezeigt.

Alle gelöschten Endpunkte sind im Ordner **Gelöscht** gespeichert. Weitere Informationen finden Sie unter „[Endpunkte aus dem Netzwerkinventar löschen](#)“ (S. 218).

Beachten Sie

Sie können nur diejenigen Gruppen verwalten, für die Sie Administratorrechte haben.

2. Im rechten Fenster wird der Inhalt der Gruppe angezeigt, die Sie im linken Fenster ausgewählt haben. Dieses Fenster besteht aus einem Raster, in dem in jeder Zeile ein Netzwerkobjekt steht und in jeder Spalte bestimmte Informationen zu diesen Objekten.

In diesem Fenster können Sie Folgendes tun:

- Detaillierte Informationen zu jedem Netzwerkobjekt in Ihrem Konto einsehen. Der Status jedes Objekts wird durch das Symbol neben seinem Namen angezeigt. Bewegen Sie den Mauszeiger über das Symbol, um einen Tooltip mit weiteren Informationen anzuzeigen. Klicken Sie auf den Namen des Objekts, um ein Fenster mit weiteren Informationen anzuzeigen.

Jede Art von Objekt, z. B. Computer, virtuelle Maschine oder Ordner, wird durch ein bestimmtes Symbol dargestellt. Jedes Netzwerkobjekt hat außerdem einen bestimmten Status in Bezug auf Verwaltungszustand, Sicherheitsprobleme, Netzwerkverbindung usw. Nähere Details zur Beschreibung jedes Netzwerkobjektsymbols und der jeweiligen Zustände finden Sie unter „[Netzwerkobjekttypen und -status](#)“ (S. 543).

- Über die [Symbolleiste](#) am oberen Rand der Tabelle können Sie bestimmte Operationen für jedes Netzwerkobjekt ausführen (z. B. Aufgaben ausführen, Berichte erstellen, Richtlinien zuweisen und löschen) und die Tabellendaten [neu laden](#).
3. Mit der [Ansichtsauswahl](#) am oberen Rand der Netzwerkfenster können Sie zwischen verschiedenen Inhalten des Netzwerkinventars hin und her schalten und so nur bestimmte gewünschte Endpunkttypen anzeigen.
 4. Über das **Filter**-Menü oben im Netzwerkfenster können Sie mithilfe verschiedener Filterkriterien die Anzeige auf bestimmte Netzwerkobjekte beschränken. Die Optionen des **Filter**-Menüs beziehen sich auf die aktuell gewählte Netzwerkansicht.

Im Bereich **Netzwerk** können Sie auch die Installationspakete sowie die Aufgaben für jeden Netzwerkobjekttyp verwalten.



Beachten Sie

Weitere Informationen zu Installationspaketen finden Sie in der GravityZone-Installationsanleitung.

Weitere Informationen zu Netzwerkobjekten finden Sie unter:

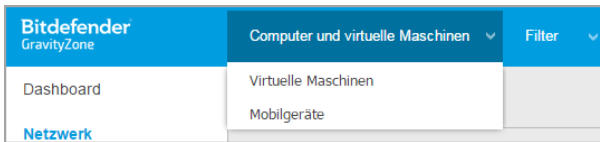
- „[Mit Netzwerkansichten arbeiten](#)“ (S. 46)
- „[Computer](#)“ (S. 49)

- „Virtuelle Maschinen“ (S. 109)
- „Mobilgeräte“ (S. 172)
- „Patch-Inventar“ (S. 205)
- „Aufgaben anzeigen und verwalten“ (S. 214)
- „Endpunkte aus dem Netzwerkinventar löschen“ (S. 218)
- „Konfigurieren von Netzwerkeinstellungen“ (S. 219)
- „Konfigurieren von Security Server-Einstellungen“ (S. 222)
- „Zugangsdaten-Manager“ (S. 223)

6.1. Mit Netzwerkansichten arbeiten

Die verschiedenen Endpunkttypen in Control Center werden auf der Seite **Netzwerk** unter verschiedenen Netzwerkansichten gruppiert. Jede Netzwerkansicht zeigt eine bestimmte Art von Netzwerkinfrastruktur, sprich: einen bestimmten Endpunkttyp, an.

Links oben auf der Seite **Netzwerk** können Sie über die Ansichtsauswahl die Netzwerkansicht wechseln:




Die Ansichtsauswahl

Die folgende Netzwerkansichten stehen zur Auswahl:

- [Computer und virtuelle Maschinen](#)
- [Virtuelle Maschinen](#)
- [Mobilgeräte](#)

6.1.1. Computer und virtuelle Maschinen

Diese Ansicht ist für in Active Directory integrierte Computer und virtuelle Maschinen gedacht und bietet bestimmte [Aktionen](#) und [Filterungsoptionen](#) zur Verwaltung der Computer in Ihrem Netzwerk. Steht eine Active-Directory-Integration zur Verfügung, wird der Active-Directory-Baum zusammen mit den entsprechenden Endpunkten geladen.

Während Sie in der Ansicht **Computer und Virtuelle Maschinen** arbeiten, können Sie die Inhalte des Control Center jederzeit mit Ihrem Active Directory synchronisieren, indem Sie in der Symbolleiste auf die Schaltfläche  **Mit Active Directory synchronisieren** klicken.

Alle Computer und virtuellen Maschinen, die nicht mit Active Directory integriert sind, werden unter Benutzerdefinierte Gruppen angezeigt. Dieser Ordner kann die folgenden Typen von Endpunkten enthalten:

- Computer und virtuelle Maschinen in Ihrem Netzwerk außerhalb des Active Directory.
- Virtuelle Maschinen aus einer virtualisierten Infrastruktur in Ihrem Netzwerk.
- Security Server, die bereits auf einem Host in Ihrem Netzwerk installiert und konfiguriert sind.



Beachten Sie

Wenn eine virtualisierte Infrastruktur verfügbar ist, können Sie Security Server in der Ansicht **Virtuelle Maschinen** installieren und verwalten. Andernfalls können Security Server nur lokal auf dem Host installiert und konfiguriert werden.



Wichtig

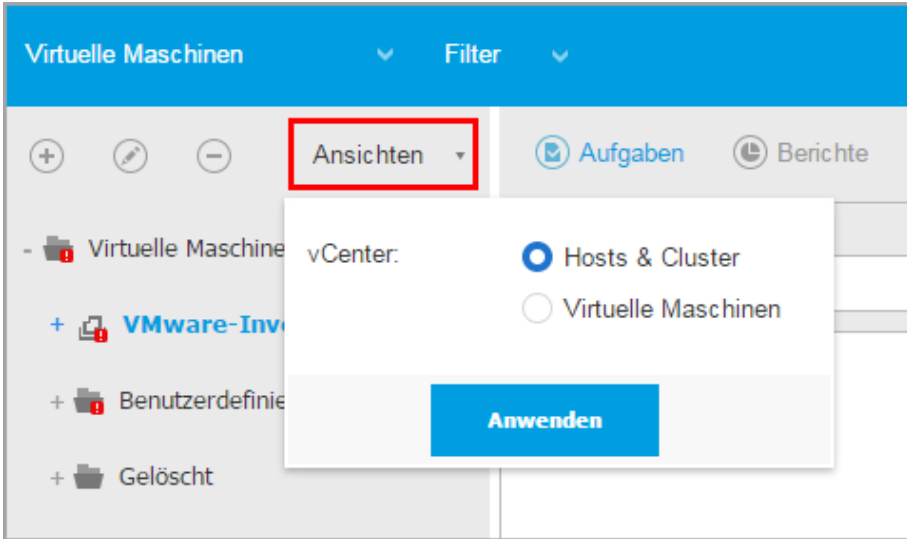
GravityZone-Administratoren mit dem Recht zur Lösungsverwaltung können die Möglichkeit, in der Ansicht **Computer und virtuelle Maschinen** virtuellen Maschinen Richtlinien zuzuweisen, einschränken. Das können sie auf der Seite **Konfiguration > Virtualisierungsanbieter** tun, wenn sie dort einen vCenter Server oder einen Xen Server konfigurieren. Weitere Informationen hierzu finden Sie im Kapitel **Schutz installieren > GravityZone-Installation und Einrichtung** der GravityZone-Installationsanleitung.

6.1.2. Virtuelle Maschinen

In dieser Ansicht werden Ihre Integrationen mit virtuellen Infrastrukturen angezeigt. Über die **Filteroptionen** in dieser Ansicht können Sie bestimmte Kriterien für die Anzeige von Entitäten der virtuellen Umgebung festlegen.

Im linken Fenster werden Ihre virtuellen Nutanix-, VMware- oder Citrix-Inventare angezeigt.

Über das Menü **Ansichten** oben im linken Fenster können Sie den Anzeigemodus der virtuellen Inventare wählen.



Die Netzwerkseite – Ansicht: virtuelle Maschinen

Alle virtuellen Maschinen in Ihrem Netzwerk, die nicht in einer virtuellen Infrastruktur integriert sind, werden unter **Benutzerdefinierte Gruppen** angezeigt.

Um auf die mit dem Control Center integrierte virtualisierte Infrastruktur zugreifen zu können, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare vCenter-Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie in vCenter Server definiert). Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht angegeben haben, müssen Sie sie angeben, sobald Sie das Inventar irgendeines vCenter-Servers durchsuchen. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

6.1.3. Mobilgeräte

In dieser Ansicht werden die Mobilgeräte in Ihrem Netzwerk angezeigt und verschiedene [Aktionen](#) und [Filteroptionen](#) zur Verwaltung bereitgestellt.

In dieser Ansicht können Sie Netzwerkentitäten nach Benutzern oder nach Geräten sortiert anzeigen.

Im Netzwerkfenster wird Ihre Active-Directory-Baumstruktur (falls vorhanden) angezeigt. In diesem Fall werden alle Active-Directory-Benutzer samt den ihnen zugewiesenen Mobilgeräten in Ihrem Netzwerkinventar angezeigt.



Beachten Sie

Die Details der Active-Directory-Benutzer werden automatisch geladen und können nicht geändert werden.

In den Benutzerdefinierten Gruppen finden sich alle Mobilgerätebenutzer, die Sie manuell zum Control Center hinzugefügt haben.

6.2. Computer

Sie können die Computer in Ihrem Konto anzeigen, indem Sie zur Seite **Netzwerk** gehen und **Computer und Virtuelle Maschinen** aus der **Ansichtsauswahl** auswählen.

Im linken Fenster sehen Sie die verfügbare Netzwerkstruktur und im rechten Fenster Details zu jedem Endpunkt.


Zunächst werden alle in Ihrem Netzwerk gefundenen Computer und virtuellen Maschinen als **nicht verwaltet** angezeigt, damit Sie per Fernzugriff die Sicherheitssoftware auf ihnen installieren können.

So passen Sie die Computerdetails an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **III Spalten** auf der rechten Seite der **Symboleiste**.
2. Wählen Sie die Spalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um zur Standardansicht zurückzukehren.

Auf der Seite **Netzwerk** stehen Ihnen folgende Verwaltungsoptionen für Computer zur Verfügung:

- [Überprüfen Sie den Status des Computers](#)
- [Computer-Details anzeigen](#)
- [Computer in Gruppen organisieren](#)
- [Sortieren, filtern und suchen](#)
- [Patches verwalten](#)
- [Aufgaben ausführen](#)
- [Schnellberichte erstellen](#)
- [Regeln zuweisen](#)
- [Mit Active Directory synchronisieren](#)

Um die neuesten Informationen in der Tabelle anzuzeigen, klicken Sie im unteren linken Bereich der Tabelle auf  **Neu laden**. Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

6.2.1. Überprüfen Sie den Status des Computers

Jeder Computer wird auf der Netzwerkseite seinem Typ und Status entsprechend durch ein Symbol dargestellt.





Unter „[Netzwerkobjekttypen und -status](#)“ (S. 543) finden Sie eine Liste aller Symbole und Status.

Detaillierte Statusinformationen finden Sie unter:

- [Verwaltungsstatus](#)
- [Verbindungsstatus](#)
- [Sicherheitsstatus](#)



Verwaltungsstatus

Computer haben immer einen der folgenden Verwaltungsstatus:

-  **Verwaltet** - Computer, auf denen der Sicherheitsagent installiert ist.
-  **Neustart steht aus** - Endpunkte, die nach Installation oder Aktualisierung von Bitdefender einen Systemneustart erfordern.
-  **Nicht verwaltet** - gefundene Computer, auf denen der Sicherheitsagent noch nicht installiert wurde.
-  **Gelöscht** - Computer, die Sie aus der Control Center gelöscht haben. Weitere Informationen finden Sie unter „[Endpunkte aus dem Netzwerkinventar löschen](#)“ (S. 218).

Verbindungsstatus

Der Verbindungsstatus betrifft nur verwaltete Computer. In dieser Hinsicht können verwaltete Computer entweder online oder offline sein:

-  **Online**. Ein blaues Symbol zeigt an, dass der Computer online ist.
-  **Offline**. Ein graues Symbol zeigt an, dass der Computer offline ist.

Ein Computer gilt als offline, wenn der Sicherheitsagent länger als 5 Minuten inaktiv ist. Mögliche Gründe, warum Computer als offline angezeigt werden:

- Der Computer ist ausgeschaltet, im Ruhezustand oder im Energiesparmodus.

**Beachten Sie**

Computer werden auch dann als online angezeigt, wenn sie gesperrt sind oder der Benutzer sich abgemeldet hat.

- Der Sicherheitsagent hat keine Verbindung zum GravityZone-Kommunikationsserver:
 - Die Verbindung des Computers zum Netzwerk könnte unterbrochen worden sein.
 - Eine Netzwerk-Firewall oder ein Router könnte die Kommunikation zwischen dem Sicherheitsagenten und dem GravityZone-Kommunikationsserver blockieren.
 - Der Computer befindet sich hinter einem Proxy-Server, und in der zugewiesenen Richtlinie wurden die Proxy-Einstellungen nicht korrekt konfiguriert.

**Warnung**

Bei Computern hinter einem Proxy-Server müssen die Proxy-Einstellungen im Installationspaket des Sicherheitsagenten korrekt konfiguriert sein, da der Computer sonst nicht mit der GravityZone kommunizieren kann und immer als offline angezeigt wird, selbst wenn nach der Installation [eine Richtlinie mit den korrekten Proxy-Einstellungen](#) angewendet wird.

- Der Sicherheitsagent funktioniert unter Umständen nicht richtig.

So finden Sie heraus, wie lange Computer inaktiv waren:

1. Zeigen Sie nur die verwalteten Computer an. Klicken Sie am oberen Rand der Tabelle auf das Menü **Filter**, wählen Sie im Reiter **Sicherheit** alle gewünschten "Verwaltet"-Optionen, markieren Sie dann im Reiter **Tiefe** die Option **Alle Objekte rekursiv** und klicken Sie anschließend auf **Speichern**.
2. Klicken Sie auf die Spaltenüberschrift **Zuletzt gesehen**, um die Computer nach dem Zeitraum ihrer Inaktivität zu sortieren.

Sie können kürzere Inaktivitätszeiträume (Minuten, Stunden) ignorieren, da diese vermutlich auf ein temporäres Problem zurückzuführen sind. Der Computer ist zum Beispiel gerade ausgeschaltet.

Längere Inaktivitätszeiträume (Tage, Wochen) deuten in der Regel auf ein Problem mit dem Computer hin.





Beachten Sie

Wir empfehlen, die Netzwerktabelle immer mal wieder **neu zu laden**, damit die jeweils aktuellen Daten angezeigt werden.

Sicherheitsstatus

Der Sicherheitsstatus betrifft nur verwaltete Computer. Computer mit Sicherheitsproblemen erkennen Sie daran, dass ein Warnsymbol am Statussymbol angezeigt wird:

-  Computer verwaltet, mit Problemen, online.
-  Computer verwaltet, mit Problemen, offline.

Ein Computer hat dann Sicherheitsprobleme, wenn mindestens einer der folgenden Punkte zutrifft:

- Malware-Schutz ist deaktiviert.
- Der Lizenzzeitraum ist abgelaufen.
- Der Sicherheitsagent ist veraltet.
- Die Sicherheitsinhalte sind veraltet.
- Malware wurde gefunden.
- Die Verbindung mit Bitdefender Cloud Services konnte nicht hergestellt werden.
Mögliche Gründe hierfür sind:
 - Der Computer hat Probleme mit der Internetverbindung.
 - Eine Netzwerk-Firewall blockiert die Verbindung mit Bitdefender Cloud Services.
 - Port 443, der für die Kommunikation mit Bitdefender Cloud Services verwendet wird, ist geschlossen.

In diesem Fall läuft der Malware-Schutz allein auf Grundlage der lokalen Engines. Cloud-Scans sind ausgeschaltet. Das heißt, dass der Sicherheitsagent keinen umfassenden Echtzeitschutz gewährleisten kann.

Wenn Ihnen ein Computer mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um das Fenster **Informationen** anzuzeigen. Sicherheitsprobleme erkennen Sie an diesem **!** Symbol. Vergessen Sie dabei nicht, in jedem einzelnen **Reiter der Informationseite** nach Sicherheitsinformationen zu suchen. Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen. Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.



Beachten Sie

Wir empfehlen, die Netzwerktabelle immer mal wieder **neu zu laden**, damit die jeweils aktuellen Daten angezeigt werden.

6.2.2. Anzeigen von Computerdetails

Gehen Sie folgendermaßen vor, um Details zu den einzelnen Computern auf der **Netzwerkseite** abzurufen:

- Aufrufen der **Netzwerkseite**
- Aufrufen des **Informationsfensters**

Aufrufen der Netzwerkseite

Detailinformationen zu einem Computer finden Sie auf der **Netzwerkseite** in der Tabelle im Fenster rechts.

Mit einem Klick auf die Schaltfläche **III Spalten** oben rechts im Fenster können Sie Spalten mit Endpunktinformationen hinzufügen oder entfernen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
Alle Endpunkte der gewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
4. Der Status eines Computers ist durch ein Symbol klar gekennzeichnet. Detaillierte Informationen finden Sie unter „Überprüfen Sie den Status des Computers“ (S. 50).
5. Die einzelnen Spalten enthalten verschiedene Informationen zu jedem Computer. Über die Kopfzeile können Sie je nach verfügbaren Kriterien eine inkrementelle Suche nach bestimmten Endpunkten starten:
 - **Name**: Name des Endpunkts.
 - **FQDN**: der sog. Fully Qualified Domain Name (vollständig qualifizierte Domainname), der den Host-Namen und den Domain-Namen beinhaltet.
 - **Betriebssystem**: auf dem Endpunkt installiertes Betriebssystem.
 - **IP**: IP-Adresse des Endpunktes.

- **Zuletzt gesehen:** Datum und Zeitpunkt, zu denen der Endpunkt zuletzt online gesehen wurde.



Beachten Sie

Sie sollten regelmäßig das Feld **Zuletzt gesehen** überprüfen, da lange Zeiträume der Inaktivität bedeuten können, dass Kommunikationsprobleme vorliegen oder der Computer vom Netzwerk getrennt wurde.

- **Bezeichnung:** Benutzerdefinierte Zeichenfolge mit zusätzlichen Informationen zum Endpunkt. Sie können im **Informationsfenster** eines Endpunktes eine Bezeichnung hinzufügen und Sie später in Ihren Suchen verwenden.
- **Richtlinie:** Die auf den Endpunkt angewandte Richtlinie, mit einem Link zum Anzeigen und Anpassen der Richtlinieneinstellungen.

Aufrufen des Informationsfensters

Klicken auf der **Netzwerkseite** im Fenster rechts auf den Namen des Endpunktes, den Sie im **Informationsfenster** anzeigen möchten. In diesem Fenster werden nur die für den ausgewählten Endpunkt verfügbaren Daten nach unterschiedlichen Reitern sortiert angezeigt.

Im Folgenden finden Sie die vollständige Auflistung aller Informationen, die im **Informationsfenster** zu finden sind, nach Endpunkttyp und den dazugehörigen Sicherheitsinformationen.

Reiter „Allgemein“

- Allgemeine Informationen zum Computer wie Name, FQDN-Informationen, IP-Adresse, Betriebssystem, Infrastruktur, übergeordnete Gruppe und aktueller Verbindungsstatus.

In diesem Bereich können Sie dem Endpunkt eine Bezeichnung zuweisen. So können Sie Endpunkte mit der gleichen Bezeichnung schnell und bequem finden und dort Aktionen ausführen, unabhängig davon, wo im Netzwerk sie sich befinden. Weitere Informationen zu den Endpunktfiltren finden Sie im Kapitel **„Sortieren, Filtern und Suchen von Computern“** (S. 69).

- Informationen zu den Schutzebenen, einschließlich einer Liste der Sicherheitstechnologien, die Sie mit Ihrer GravityZone-Lösung erworben haben, und ihren Lizenzstatus. Folgende Status sind möglich:

- **Verfügbar / Aktiv** – Der Lizenzschlüssel für diese Schutzebene ist auf dem Endpunkt aktiv.
- **Abgelaufen** – Der Lizenzschlüssel für diese Schutzebene ist abgelaufen.
- **Ausstehend** – der Lizenzschlüssel wurde noch nicht bestätigt.



Beachten Sie

Weitere Informationen zu den Schutzebenen finden Sie im Reiter **Schutz**.

- **Relaisverbindung:** Der Name, die IP und die Bezeichnung des Relais, mit dem der Endpunkt ggf. verbunden ist.

Informationen
✕

Allgemein Schutz Richtlinie Scan-Protokolle

Computer	Schutzebenen
Name: 192_168_2_251	Endpunkt: Aktiv
FQDN: 192_168_2_251	
IP: 10.17.47.155	
Betriebssystem: Windows Server 2008 R2 Enterprise	
Bezeichnung: <input style="width: 100%;" type="text"/>	
Infrastruktur: Benutzerdefinierte Gruppen	
Gruppe: Custom Groups	
Zustand: Offline	
Zuletzt gesehen: 23 Oktober 2017, 06:53:17	

Speichern
Schließen


Fenster Informationen - Reiter Allgemein


Reiter Schutz

In diesem Reiter finden Sie Details zu dem auf dem Endpunkt angewandten Schutz. Diese beziehen sich auf:

- Informationen zum Sicherheitsagenten wie Produktname, Version, Update-Status und Update-Adressen sowie die Konfiguration der Scan-Engines und Versionen der Sicherheitsinhalte. Im Falle vom Exchange-Schutz ist auch die Version der Spam-Schutz-Engine verfügbar.
- Sicherheitsstatus für jede Schutzebene. Dieser Status wird rechts neben dem Namen der Schutzebene angezeigt:

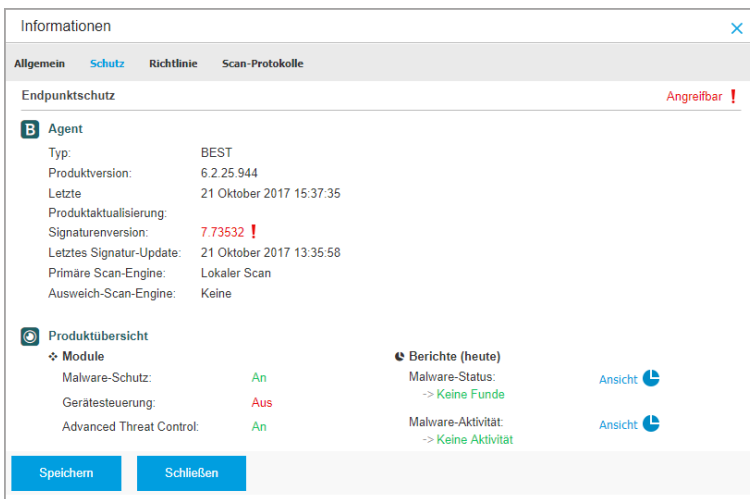
- **Sicher**, d. h. auf den Endpunkten, auf denen die Schutzebene angewandt wird, liegen keine Sicherheitsprobleme vor.
- **Angreifbar**, d. h. auf den Endpunkten, auf denen die Schutzebene angewandt wird, liegen Sicherheitsprobleme vor. Weitere Informationen finden Sie unter „Sicherheitsstatus“ (S. 52).
- Zugehörige Security Server. Jeder zugewiesene Security Server wird bei agentenlosen Installationen angezeigt oder dann, wenn die Scan-Engines der Sicherheitsagenten für die Verwendung vom Remote-Scan konfiguriert wurden. Security Server-Informationen helfen bei der Identifikation der virtuellen Appliance und dem Einholen des Update-Status.
- Status der Sicherheitsmodule. Hier sehen Sie, welche Sicherheitsmodule auf dem Endpunkt installiert wurden, und welchen Status die verfügbaren Module (**Ein/Aus**) gemäß der angewendeten Richtlinie haben.
- Ein schneller Überblick über die Modulaktivität und Malware-Berichte des aktuellen Tages.

Klicken Sie auf den  **Anzeigen**-Link, um die Berichtsoptionen anzuzeigen und den Bericht anzulegen. Weitere Informationen finden Sie unter „[Berichte erstellen](#)“ (S. 459)

- Informationen zum Sandbox Analyzer:
 - Sandbox Analyzer-Verwendungsstatus auf dem Endpunkt, wird rechts im Fenster angezeigt:
 - **Aktiv**: Der Sandbox Analyzer ist lizenziert (verfügbar) und wurde per Richtlinie auf dem Endpunkt aktiviert.
 - **Inaktiv**: Der Sandbox Analyzer ist lizenziert (verfügbar), wurde aber nicht per Richtlinie auf dem Endpunkt aktiviert.
 - Name des Agenten, der als Einspeisungssensor fungiert.
 - Modulstatus auf dem Endpunkt:
 - **An** - Der Sandbox Analyzer wurde per Richtlinie auf dem Endpunkt aktiviert.
 - **Aus** - Der Sandbox Analyzer wurde nicht per Richtlinie auf dem Endpunkt aktiviert.
 - Bedrohungsfunde in der letzten Woche (über einen Klick auf  **Ansicht** zur Anzeige des Berichts).

- Weitergehende Informationen zum Verschlüsselungsmodul, darunter:
 - Gefundene Laufwerke (mit Kennzeichnung des Boot-Laufwerks)
 - Verschlüsselungsstatus für jedes Laufwerk (also **Verschlüsselt, Verschlüsselung wird durchgeführt, Entschlüsselung wird durchgeführt, Nicht verschlüsselt, Verriegelt** oder **Angehalten**).

Klicken Sie auf den Link **Wiederherstellung**, um den Wiederherstellungsschlüssel für das entsprechende verschlüsselte Laufwerk abzurufen. Weitere Details zum Abrufen von Wiederherstellungsschlüsseln finden Sie hier: „“ (S. 107).
- Status der Sicherheitstelemetrie, der Sie darüber informiert, ob die Verbindung zwischen dem Endpunkt und dem SIEM-Server hergestellt wurde und funktioniert, deaktiviert ist oder Probleme aufweist.



Fenster Informationen - Reiter Schutz

Reiter Richtlinie

Auf einem Endpunkt können mehrere Richtlinien angewandt werden, es kann jedoch immer nur eine der Richtlinien aktiv sein. Im Reiter **Richtlinie** werden Informationen zu allen Richtlinien angezeigt, die auf den Endpunkt angewandt wurden.

- Name der aktiven Richtlinie. Klicken Sie auf den Namen der Richtlinie, um die Richtlinienvorlage und ihre Einstellungen anzuzeigen.
- Der aktive Richtlinientyp, möglich sind:
 - **Gerät**, d. h. die Richtlinie wurde dem Endpunkt von Netzwerkadministrator manuell zugewiesen.
 - **Standort**, d. h. eine regelbasierte Richtlinie, die dem Endpunkt automatisch zugewiesen wird, wenn die Netzwerkeinstellungen des Endpunktes mit den Bedingungen einer bestehenden **Zuweisungsregel** übereinstimmen.
Ein Laptop hat z.B. zwei standortbezogene Richtlinien: eine namens **Büro**, die aktiv wird, wenn sie mit dem Firmen-LAN verbunden ist, eine zweite namens **Roaming**, die aktiv wird, wenn der Benutzer extern arbeitet und mit anderen Netzwerken verbunden ist.
 - **Benutzer**, d. h. eine regelbasierte Richtlinie, die dem Endpunkt automatisch zugewiesen wird, wenn dieser mit dem Active-Directory-Ziel übereinstimmt, das mit einer bestehenden Zuweisungsregel festgelegt wurde.
 - **Extern (NSX)**, d. h. die Richtlinie ist in der VMware-NSX-Umgebung definiert.
- Der aktive Richtlinienzuweisungstyp, möglich sind:
 - **Direkt**, d. h. die Richtlinie wird direkt auf den Endpunkt angewandt.
 - **Geerbt**, d. h. der Endpunkt erbt die Richtlinie von einer übergeordneten Gruppe.
- **Anzuwendende Richtlinien**: Zeigt die Liste der Richtlinien an, die mit bestehenden Zuweisungsregeln verknüpft sind. Diese Richtlinien werden unter Umständen auf den Endpunkt angewandt, wenn dieser mit den Bedingungen der verknüpften Zuweisungsregeln übereinstimmt.

Informationen
✕

Allgemein Schutz Richtlinie Scan-Protokolle

Details

Aktive Richtlinie: rv

Typ: Gerät

Zuweisung: Direkt

Zugewiesene Regeln

Name der Richtlinie	Status	Typ	Zuweisungsregeln
rv	Angewendet	Gerät	N/A

Erste Seite ← Seite 1 von 1 → Letzte Seite 20

1 Objekt(e)

Speichern
Schließen

Fenster Informationen - Reiter Richtlinie

Weitere Informationen zu den Richtlinien finden Sie unter „[Richtlinieneinstellungen ändern](#)“ (S. 242)

Reiter Verbundene Endpunkte

Der Reiter **Verbundene Endpunkte** ist nur für Endpunkte mit Relais-Rolle verfügbar. In diesem Reiter werden Informationen über Endpunkte angezeigt, die mit dem Relais verbunden sind, z. B. Name, IP-Adresse und Bezeichnung.

Informationen
✕

Allgemein Schutz Richtlinie Relais Scan-Protokolle

Verbundene Endpunkte

Endpunkt-Name	IP	Bezeichnung
CONN-BD	192.168.12.101	
CONN-WIN	192.168.12.222	

Erste Seite ← Seite 0 von 0 → Letzte Seite 20

0 Objekte

Speichern
Schließen

Informationsfenster - Reiter Verbundene Endpunkte

Reiter Repository-Details

Der Reiter **Repository-Details** ist nur für Endpunkte mit Relais-Rolle verfügbar und liefert Informationen über Updates des Sicherheitsagenten und die Sicherheitsinhalte.

Der Reiter zeigt Details über die auf dem Relais gespeicherten und im offiziellen Repository verfügbaren Produkt- und Signaturversionen, Update-Ringe, Datum und Uhrzeit des Updates sowie die letzte Überprüfung auf neue Versionen.

< Back
AST-TB-W7X86-2

General
Protection
Policy
Connected Endpoints
Repository details
Scan Logs
Troubleshooting

Bitdefender Endpoint Security Tools

BEST (Windows)

Product version (stored locally)

Slow ring:	6.6.18.265
Fast ring:	6.6.19.273

Product version (Bitdefender repository)

Slow ring:	N/A
Fast ring:	N/A

Last update time: 26 June 2020 18:4...

Last check time: N/A

Security Content

FULL ENGINES (Local Scan)

Signatures stored locally

x86:	7.84969
x64:	N/A

Signatures in Bitdefender repository

x86:	7.84969
x64:	N/A

Last update time: 29 June 2020 14:5...

Last check time: 29 June 2020 16:0...

Status: ● Up to date

LIGHT ENGINES (Hybrid Scan)

Signatures stored locally

x86:	N/A
x64:	7.84969

Signatures in Bitdefender repository

x86:	N/A
x64:	7.84969

Last update time: 29 June 2020 14:5...

Last check time: 29 June 2020 16:0...

Status: ● Up to date

Informationsfenster - Reiter Repository-Details

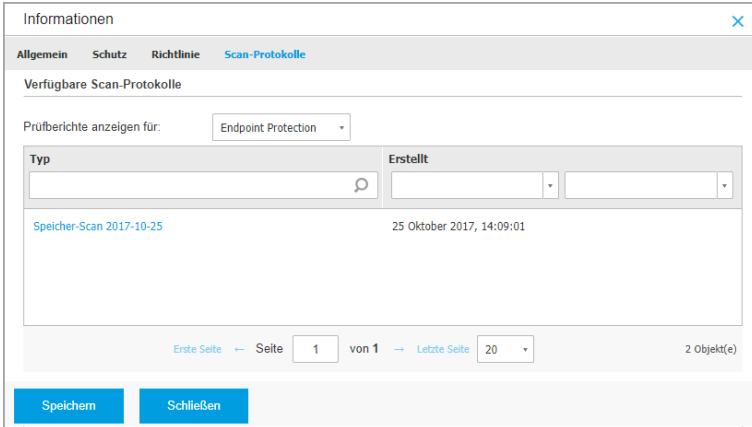
Reiter Scan-Protokolle

Im Reiter **Scan-Protokolle** werden detaillierte Informationen zu allen Scan-Aufgaben angezeigt, die auf dem Endpunkt ausgeführt wurden.

Protokolle werden nach Schutzebene geordnet. Über das Klappenmenü können Sie entscheiden, für welche Ebene Protokolle angezeigt werden sollen.

Klicken Sie auf die gewünschte Scan-Aufgabe, um das Protokoll in einem neuen Reiter im Browser zu öffnen.

Wenn mehrere Scan-Protokolle zur Verfügung stehen, können Sie sich über mehrere Seiten erstrecken. Über die Navigation am unteren Rand der Tabelle können Sie zwischen den Seiten wechseln. Wenn Sie sehr viele Einträge haben, können Sie die Filteroptionen über der Tabelle nutzen.



Fenster Informationen - Reiter Scan-Protokolle

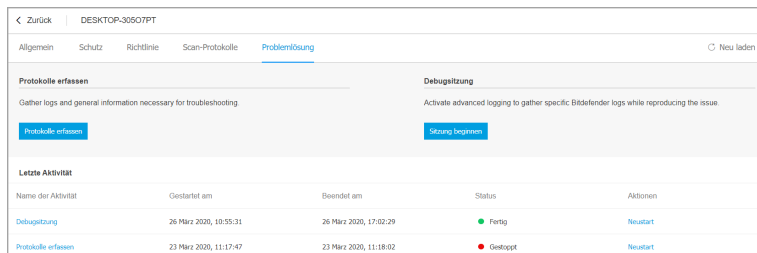
Reiter Problemlösung

Dieser Abschnitt befasst sich mit der Behebung von Problemen mit dem Agenten. Sie können allgemeine oder spezifische Protokolle aus der Endpunktprüfung sammeln oder Maßnahmen zur aktuellen Problembehebungsereignissen ergreifen und frühere Aktivitäten anzeigen.



Wichtig

Die Fehlerbehebung ist für Windows-, Linux-, macOS- und alle Arten von Security Servern verfügbar.



Informationsfenster - Reiter Problemlösung

● Protokolle erfassen

Mit dieser Option können Sie eine Reihe von Protokollen und allgemeinen Informationen sammeln, die für die Problembekämpfung erforderlich sind, wie z. B. Einstellungen, aktive Module oder angewandte Richtlinien des Zielcomputers. Alle generierten Daten werden in einem Archiv gespeichert.

Es wird empfohlen, die Option zu verwenden, wenn die Ursache eines Problems unklar ist.

So können Sie den Problembekämpfung starten:

1. Klicken Sie auf die Schaltfläche **Protokolle erfassen**. Ein Konfigurationsfenster wird geöffnet.
2. Wählen Sie im Abschnitt **Protokollspeicher** einen Speicherort aus.
 - **Zielcomputer**: Das Protokollarchiv wird am angegebenen lokalen Pfad gespeichert. Für Security Server kann dieser Pfad nicht konfiguriert werden.
 - **Netzwerkfreigabe**: Das Protokollarchiv wird am angegebenen Pfad auf der Netzwerkfreigabe gespeichert.

Mit der Option **Protokolle auch auf dem Zielcomputer speichern** können Sie eine Kopie des Protokollarchivs als Backup auf dem betroffenen Computer speichern.

3. Geben Sie abhängig vom ausgewählten Speicherort die erforderlichen Informationen (lokaler Pfad, Anmeldeinformationen für die Netzwerkfreigabe, Pfad zum freigegebenen Speicherort) ein.
4. Klicken Sie auf die Schaltfläche **Protokolle erfassen**.

● Debugsituation

Mit der Debugsitzung können Sie die erweiterte Protokollierung auf dem Zielcomputer aktivieren, um spezifische Protokolle zu erstellen, während das Problem reproduziert wird.

Sie sollten diese Option verwenden, wenn Sie bereits wissen, welches Modul Probleme verursacht, oder wenn Ihnen dies vom Bitdefender-Enterpris-Support empfohlen wird. Alle generierten Daten werden in einem Archiv gespeichert.

So können Sie den Problembhebung starten:

1. Klicken Sie auf die Schaltfläche **Sitzung beginnen**. Ein Konfigurationsfenster wird geöffnet.
2. Wählen Sie im Abschnitt **Problemtyp** das Problem aus, das Ihrer Vermutung nach vorliegt:

Problemtypen bei Windows- und macOS-Maschinen:

Problemart	Anwendungsfall
Malware-Schutz (Zugriff- und Bedarf-Scans)	<ul style="list-style-type: none"> - Allgemeine Verlangsamung des Endpunkts - Die Antwort eines Programms oder einer Systemressource dauert zu lange - Ein Scanvorgang dauert länger als üblich - Keine Verbindung zum Host-Sicherheitsdienst
Update-Fehler	<ul style="list-style-type: none"> - Bei Aktualisierungen des Produkts oder von Sicherheitsinhalten empfangene Fehlermeldungen
Inhaltssteuerung (Datenverkehr-Scan und Benutzersteuerung)	<ul style="list-style-type: none"> - Website lädt nicht - Elemente der Webseite werden nicht richtig angezeigt
Konnektivität der Cloud-Dienste	<ul style="list-style-type: none"> - Der Endpunkt hat keine Verbindung zu den Bitdefender Cloud-Diensten
Allgemeine Produktprobleme (ausführliche Protokolle)	<ul style="list-style-type: none"> - Reproduktion eines generischen gemeldeten Problems mit der ausführlichen Protokollierung


Problemtypen bei Linux-Maschinen:




Problemart	Anwendungsfall
Malware-Schutz und Update	<ul style="list-style-type: none"> - Ein Scanvorgang dauert länger als üblich und verbraucht mehr Ressourcen - Bei Aktualisierungen des Produkts oder von Sicherheitsinhalten empfangene Fehlermeldungen - Der Endpunkt kann keine Verbindung zur GravityZone-Konsole herstellen.
Allgemeine Produktprobleme (ausführliche Protokolle)	<ul style="list-style-type: none"> - Reproduktion eines generischen gemeldeten Problems mit der ausführlichen Protokollierung

Problemtypen bei Security-Servern:

Problemart	Anwendungsfall
Malware-Schutz (Zugriff- und Bedarf-Scans)	<p>Sämtliches unerwartetes Verhalten des Security-Servers, d. h.:</p> <ul style="list-style-type: none"> - Virtuelle Maschinen sind nicht vollständig geschützt. - Malware-Scans werden nicht ausgeführt oder dauern länger, als erwartet - Produkt-Updates werden nicht ordnungsgemäß installiert - Generische Security-Server-Fehlfunktion (BD-Daemons laufen nicht)
Kommunikation mit dem GravityZone-Control-Center	<p>Sämtliches in der GravityZone-Konsole beobachtetes unerwartetes Verhalten:</p> <ul style="list-style-type: none"> - Virtuelle Maschinen werden in GravityZone nicht ordnungsgemäß gemeldet - Probleme mit Richtlinien (Richtlinie nicht angewendet) - Der Security Server kann keine Verbindung mit der GravityZone-Konsole herstellen

Problemart	Anwendungsfall
	 <p>Beachten Sie Setzen Sie diese Methode nur auf E m p f e h l u n g des Bitdefender-Enterprise-Supports ein.</p>


3. Wählen Sie unter **Dauer der Debugsitzung** das Zeitintervall, nach dem die Debugsitzung automatisch beendet wird.

 **Beachten Sie**
Es wird empfohlen, die Sitzung mit der Option **Sitzung abschließen** manuell zu beenden, sobald Sie das Problem reproduziert haben.

4. Wählen Sie im Abschnitt **Protokollspeicher** einen Speicherort aus.
 - **Zielcomputer:** Das Protokollarchiv wird am angegebenen lokalen Pfad gespeichert. Für Security Server kann dieser Pfad nicht konfiguriert werden.
 - **Netzwerkfreigabe:** Das Protokollarchiv wird am angegebenen Pfad auf der Netzwerkfreigabe gespeichert.

Mit der Option **Protokolle auch auf dem Zielcomputer speichern** können Sie eine Kopie des Protokollarchivs als Backup auf dem betroffenen Computer speichern.

5. Geben Sie abhängig vom ausgewählten Speicherort die erforderlichen Informationen (lokaler Pfad, Anmeldeinformationen für die Netzwerkfreigabe, Pfad zum freigegebenen Speicherort) ein.
6. Klicken Sie auf die Schaltfläche **Sitzung beginnen**.

 **Wichtig**
Sie können nur einen Problembehebungsprozess (**Protokolle erfassen / Debugsitzung**) gleichzeitig auf dem betroffenen Computer ausführen.

- **Problembehebungsverlauf**

Der Abschnitt **Letzte Aktivität** gibt einen Überblick über die Problembehebungsaktivität auf dem betroffenen Computer dar. Das Raster

zeigt nur die letzten 10 Problembehebungsereignisse in chronologisch umgekehrter Reihenfolge an und löscht automatisch Aktivitäten, die älter als 30 Tage sind.

Das Gitter zeigt die Details zu jedem Problembehebungsprozess an.

Der Prozess hat Haupt- und Zwischenstatus. Abhängig von den benutzerdefinierten Einstellungen können die folgenden Status vorliegen, für die Sie aktiv werden müssen:

- **Wird ausgeführt (Bereit, das Problem zu reproduzieren)** - Greifen Sie manuell oder per Fernzugriff auf den betroffenen Computer zu und reproduzieren Sie das Problem.

Es gibt mehrere Möglichkeiten, einen Problembehebungsprozess zu beenden:

- **Sitzung abschließen:** Beendet die Debugsitzung und den Erfassungsvorgang auf dem Zielcomputer und speichert alle gesammelten Daten am angegebenen Speicherort.

Es wird empfohlen, diese Option sofort nach der Reproduktion des Problems zu verwenden.

- **Abbrechen:** Diese Option bricht den Prozess ab und es werden keine Protokolle erfasst.

Nutzen Sie diese Option, wenn Sie keine Protokolle vom Zielcomputer erfassen möchten.

- **Beenden erzwingen:** Erzwingt das Beenden des Problembehebungsprozesses.


Verwenden Sie diese Option, wenn das Abbrechen der Sitzung zu lange dauert oder der Zielcomputer nicht reagiert und Sie in wenigen Minuten eine neue Sitzung starten können.

So starten Sie einen Problembehebungsvorgang neu:

- **Neustart:** Diese Schaltfläche befindet sich für jedes Ereignis im Bereich **Aktionen**. Über sie wird der gewählte Problembehebungsvorgang mit den bisherigen Einstellungen neu gestartet.



Wichtig

- Verwenden Sie die  **Neu laden**-Schaltfläche oben rechts auf der Seite **Problemlösung**, um sicherzustellen, dass die Konsole die neuesten Informationen anzeigt.

- Um weitere Details zu einem bestimmten Ereignis zu erhalten, klicken Sie im Raster auf den Namen des Ereignisses.

6.2.3. Computer in Gruppen organisieren

Sie können Computergruppen im linken Fenster der Seite **Netzwerk** verwalten.

Ein großer Vorteil dieser Funktion ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Von Active Directory importierte Computer werden im Ordner **Active Directory** zusammengefasst. Die Active-Directory-Gruppen können sie nicht bearbeiten. Sie können nur die zugehörigen Computer anzeigen und verwalten.

Alle in Ihrem Netzwerk gefundenen Computer außerhalb des Active Directory werden unter **Benutzerdefinierte Gruppen** sortiert. Dort können Sie sie beliebig in Gruppen organisieren. Unter **Benutzerdefinierte Gruppen** können Sie Computergruppen innerhalb einer benutzerdefinierten Baumstruktur [erstellen](#), [löschen](#), [umbenennen](#) und [verschieben](#).



Beachten Sie

- Eine Gruppe kann sowohl Computer als auch andere Gruppen enthalten.
- Wenn Sie im linken Bereich eine Gruppe auswählen, können Sie alle enthaltenen Computer einsehen - ausgenommen der, die in die jeweiligen Untergruppen eingeordnet wurden. Wenn Sie alle Computer der Gruppe und ihrer Untergruppen anzeigen möchten, klicken Sie auf das Menü **Filter** am oberen Rand der Tabelle und wählen Sie **Alle Objekte rekursiv** im Bereich **Tiefe**.

Gruppen erstellen

Bevor Sie Gruppen erstellen, sollten Sie sich überlegen, warum Sie diese Gruppen brauchen und sie dann nach einem bestimmten System erstellen. Sie können Endpunkte zum Beispiel anhand von einem oder einer Kombination der folgenden Kriterien in Gruppen einteilen:

- Organisationsstruktur (Vertrieb, Marketing, Qualitätssicherung, Software-Entwicklung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Um Ihr Netzwerk in Gruppen aufzuteilen:

1. Wählen Sie **Benutzerdefinierte Gruppen** im linken Fenster.
2. Klicken Sie auf die Schaltfläche **+** **Gruppe hinzufügen** im oberen Bereich des linken Fensters.
3. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK**. Die neue Gruppe wird im Ordner **Benutzerdefinierte Gruppen** angezeigt.

Gruppen umbenennen

So benennen Sie eine Gruppe um:

1. Wählen Sie im linken Fenster die Gruppe aus.
2. Klicken Sie auf die Schaltfläche **✎** **Gruppe bearbeiten** im oberen Bereich des linken Fensters.
3. Geben Sie den neuen Namen in das entsprechende Feld ein.
4. Klicken Sie zur Bestätigung auf **OK**.

Gruppen und Computer verschieben

Sie können Entitäten irgendwo innerhalb der Gruppenhierarchie nach **Benutzerdefinierte Gruppen** verschieben. Ziehen Sie die gewünschte Entität einfach mit der Maus aus dem rechten Fenster in die gewünschte Gruppe im linken Fenster.



Beachten Sie

Die Entität, die verschoben wird, erbt die Richtlinieneinstellungen der neuen übergeordneten Gruppe, sofern ihr keine abweichende Richtlinie direkt zugewiesen wurde. Weitere Informationen über Richtlinienvererbung finden Sie unter „[Sicherheitsrichtlinien](#)“ (S. 227).

Gruppen löschen

Eine Gruppe zu löschen ist eine unwiderrufliche Aktion. Das bewirkt, dass der auf dem entsprechenden Endpunkt installierte Sicherheitsagent entfernt wird.

Um eine Gruppe zu löschen:

1. Klicken Sie auf die leere Gruppe im linken Fenster der Seite **Netzwerk**.
2. Klicken Sie auf die Schaltfläche **-** **Gruppe entfernen** im oberen Bereich des linken Fensters. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

6.2.4. Sortieren, Filtern und Suchen von Computern

Abhängig von der Anzahl der Endpunkte kann sich die Tabelle im rechten Fenster über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt). Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Bei zu vielen Einträgen können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das **Filter**-Menü im oberen Bereich der Tabelle verwenden, um nur die Einträge anzuzeigen, die Sie interessieren. So können Sie zum Beispiel nach einem bestimmten Computer suchen oder nur verwaltete Computer anzeigen.

Computer sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Wenn Sie zum Beispiel möchten, dass die Computer nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**. Wenn Sie erneut auf den Titel klicken, werden die Computer in umgekehrter Reihenfolge angezeigt.

Name	Betriebssystem	IP	Zuletzt gesehen	Bezeichnung
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Computer sortieren

Computer filtern

Ihre Netzwerkentitäten können Sie filtern, indem Sie im oberen Bereich der Netzwerkfenster das **Filter**-Menü verwenden.

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Klicken Sie auf das **Filter**-Menü im oberen Bereich der Netzwerkfenster.
3. So verwenden Sie die Filterkriterien:
 - **Typ**. Wählen Sie die Art der Entitäten aus, die angezeigt werden sollen (Computer, virtuelle Maschinen, Ordner).



Typ	Sicherheit	Richtlinie	Tiefe
Filtern nach			
<input type="checkbox"/> Computer			
<input type="checkbox"/> Virtuelle Maschinen			
<input type="checkbox"/> Gruppen/Ordner			
Tiefe: in den ausgewählten Ordnern			
Speichern		Abbrechen	
Zurücksetzen			

Computer - nach Art filtern

- **Sicherheit.** Zeigen Sie Computer nach Schutzverwaltung, Sicherheitsstatus oder ausstehender Aktivität an.

Typ	Sicherheit	Richtlinie	Tiefe
Verwaltung		Sicherheitsprobleme	
<input type="checkbox"/> Verwaltet(Endpunkte)		<input type="checkbox"/> Mit Sicherheitsproblemen	
<input type="checkbox"/> Verwaltet (Exchange Server)		<input type="checkbox"/> Ohne Sicherheitsprobleme	
<input type="checkbox"/> Verwaltet (Relais)			
<input type="checkbox"/> Security Server			
<input type="checkbox"/> Nicht verwaltet			
Tiefe: in den ausgewählten Ordnern			
Speichern		Abbrechen	
Zurücksetzen			

Computer - nach Sicherheit filtern

- **Richtlinie.** Wählen Sie die Richtlinienvorlage, nach der Sie die Computer filtern möchten, den Richtlinienzuweisungstyp (direkt oder geerbt) sowie den Richtlinienzuweisungsstatus (aktiv, angewendet oder ausstehend). Sie können auch nur diejenigen Entitäten anzeigen, die Richtlinien haben, die im Power-User-Modus bearbeitet wurden.

Computer - nach Richtlinie filtern

- Tiefe.** Bei der Verwaltung eines Netzwerks mit Baumstruktur werden Computer, die sich in Untergruppen befinden, bei Auswahl der Stammgruppe nicht angezeigt. Wählen Sie **Alle Objekte rekursiv**, um alle Computer der aktuellen Gruppe und alle ihre Untergruppen anzuzeigen.

Computer - nach Tiefe filtern

Wenn Sie alle Objekte rekursiv anzeigen, zeigt das Control Center sie in einer einfachen Liste an. Um den Speicherort eines Objekts zu finden, klicken Sie auf das gewünschte Objekt und dann auf die Schaltfläche **Zum Container** oberhalb der Liste. Sie werden dann zum übergeordneten Container des ausgewählten Objekts weitergeleitet.



Beachten Sie

Die ausgewählten Filterkriterien werden im unteren Teil des **Filter**-Fensters angezeigt.

Klicken Sie auf **Zurücksetzen**, um alle Filter zu löschen.

4. Klicken Sie auf **Speichern**, um die Computer nach den gewählten Kriterien zu filtern. Der Filter bleibt aktiv in der **Netzwerk**-Übersicht, bis Sie sich abmelden oder den Filter löschen.

Nach Computern suchen

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Geben Sie den Suchbegriff in das entsprechende Feld unter der Spaltenüberschrift im rechten Fenster rein. Geben Sie zum Beispiel die IP-Adresse des Computers, den Sie suchen, in das Feld **IP** ein. Nur der passende Computer wird in der Tabelle angezeigt.

Leeren Sie das Suchfeld, um die vollständige Liste der Computer anzuzeigen.

Name	FQDN	Betriebssystem	IP	Zuletzt gesehen	Bezeichnung
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	192.168.113.1 <input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> SRV2012	srv2012.x13.local	Windows Serv...	192.168.113.1	Online	N/A

Nach Computern suchen

6.2.5. Aufgaben ausführen

Über die Seite **Netzwerk** können Sie per Fernzugriff eine Reihe administrativer Aufgaben auf Computern ausführen.

Sie haben die folgenden Möglichkeiten:

- „Scan“ (S. 73)
- „Patch-Aufgaben“ (S. 83)
- „Exchange-Scan“ (S. 86)
- „Installieren“ (S. 91)
- „Client Deinstallieren“ (S. 97)
- „Client aktualisieren“ (S. 98)
- „Client neu konfigurieren“ (S. 99)
- „Client reparieren“ (S. 100)

- „Computer neu starten“ (S. 101)
- „Netzwerkerkennung“ (S. 102)
- „Anwendungserkennung“ (S. 103)
- „Security Server aktualisieren“ (S. 103)
- „Benutzerdefiniertes Tool injizieren“ (S. 104)

Sie können Aufgaben individuell für einzelne Computer oder für Gruppen von Computern erstellen. Sie können zum Beispiel per Ferninstallation den Sicherheitsagenten auf einer Gruppe nicht verwalteter Computer installieren. Später können Sie eine Scan-Aufgabe für einen bestimmten Computer aus dieser Gruppe erstellen.

Auf jedem Computer können Sie nur kompatible Aufgaben ausführen. Wenn Sie zum Beispiel einen nicht verwalteten Computer auswählen, können Sie nur den Sicherheitsagenten installieren; alle anderen Aufgaben sind nicht verfügbar.


Bei einer Gruppe wird die ausgewählte Aufgabe nur für kompatible Computer erstellt. Wenn kein Computer der Gruppe mit der ausgewählten Aufgabe kompatibel ist, werden Sie benachrichtigt, dass die Aufgabe nicht erstellt werden konnte.

Sofort nach der Erstellung startet die Aufgabe auf Computern, die online sind. Wenn ein Computer offline ist, wird die Aufgabe ausgeführt, sobald er wieder online ist.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Scan

Um eine Scan-Aufgabe per Fernzugriff auf einem oder mehreren Computern auszuführen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer oder Gruppen, die Sie scannen möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Scan**.

Ein Konfigurationsfenster wird sich öffnen.

6. Konfigurieren Sie die Scan-Optionen:

- Im Reiter **Allgemein** können Sie den Scan-Typ auswählen und der Scan-Aufgabe einen Namen geben. Der Name dient nur dazu, dass Sie den Scan auf der Seite **Aufgaben** leicht wiederfinden.

Scan-Aufgabe

Allgemein Optionen Ziel

Details

Typ: Quick Scan

Aufgabenname: Quick Scan 2016-09-21

Aufgabe mit niedriger Priorität ausführen

Computer nach Abschluss des Scans herunterfahren

Speichern Abbrechen

Computer-Scan-Aufgabe - Konfigurieren der allgemeinen Einstellungen

Wählen Sie den gewünschten Typ aus dem Menü **Typ**:

- **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren. Dieser Scan ist so vorkonfiguriert, dass nur kritische Windows- und Linux-System-Speicherorte gescannt werden können. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenskan in Anspruch nehmen würde.

Wenn Malware oder Rootkits gefunden werden, desinfiziert Bitdefender sie automatisch. Wenn die Datei aus irgendeinem Grund nicht desinfiziert werden kann, wird sie in die Quarantäne verschoben. Dieser Art Scan ignoriert verdächtige Dateien.

- Der **Vollständige Scan** durchsucht das gesamte System nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.

Bitdefender versucht automatisch als infiziert erkannte Dateien zu desinfizieren. Sollte die Malware nicht entfernt werden können, wird sie in die Quarantäne verschoben, wo sie keinen Schaden mehr anrichten kann. Verdächtige Dateien werden ignoriert. Wenn Sie auch für verdächtige Dateien Aktionen ausführen möchten oder für infizierte Dateien andere Standardaktionen definieren möchten, führen Sie einen benutzerdefinierten Scan durch.

- **Speicher-Scan** überprüft die Programme, die im Speicher des Computers laufen.
- **Netzwerk-Scan** ist ein benutzerdefinierter Scan, mit dem Netzwerklaufwerke mithilfe des Bitdefender-Sicherheitsagenten, der auf dem ansprechenden Endpunkt installiert ist, gescannt werden können. Damit die Netzwerk-Scan-Aufgabe funktioniert, müssen folgende Voraussetzungen erfüllt sein:
 - Sie müssen die Aufgabe einem einzelnen Endpunkt in Ihrem Netzwerk zuweisen.
 - Sie müssen die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann. Die nötigen Zugangsdaten können Sie im Aufgabenfenster im Reiter **Ziel** konfigurieren.
- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Für Speicher-, Netzwerk- und benutzerdefinierte Scans stehen Ihnen zudem die folgenden Optionen zur Auswahl:

- **Aufgabe mit niedriger Priorität ausführen.** Durch Anklicken dieses Kästchens setzen Sie die Priorität des Scan-Prozesses herab und ermöglichen es anderen Programmen, schneller zu laufen. Hierdurch wird die für den Scan-Prozess benötigte Zeit verlängert.



Beachten Sie

Diese Option gilt nur für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent).

- **Computer nach Abschluss des Scans herunterfahren.** Mit diesem Kästchen schalten Sie Ihren Computer aus, sofern Sie ihn eine Zeitlang nicht nutzen wollen.



Beachten Sie

Diese Option gilt für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent) und Endpoint Security for Mac.



Beachten Sie

Diese zwei Optionen gelten nur für Bitdefender Endpoint Security Tools und Endpoint Security (Vorgängeragent).

Für benutzerdefinierte Scans müssen Sie die folgenden Einstellungen konfigurieren:

- Gehen Sie zum Reiter **Optionen**, um die Scan-Optionen festzulegen. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren. Markieren Sie dazu das Kästchen **Benutzerdefiniert** und vergrößern Sie dann den Bereich **Einstellungen**.

Scan-Aufgabe

Allgemein Optionen Ziel

Prüfoptionen

- Aggressiv Benutzerdefiniert - vom Administrator festgelegte Einstellungen

- Normal

- Tolerant

- Benutzerdefiniert

▶ Einstellungen

Speichern Abbrechen

Computer-Scan-Aufgabe - Konfiguration eines benutzerdefinierten Scans

Die folgenden Optionen stehen zur Verfügung:

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateiendung), oder nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten,

durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

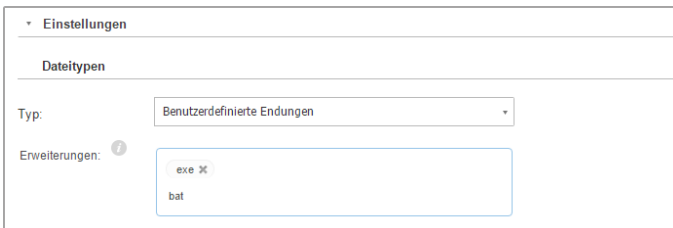
Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 545).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf **Speichern**.

Wichtig

Bitdefender-Sicherheitsagenten, die auf Windows- und Linux-Systemen installiert sind, scannen die meisten ISO-Formate, führen aber keine Aktionen für sie durch.



The screenshot shows the 'Einstellungen' (Settings) window with the 'Dateitypen' (File Types) section expanded. Under 'Typ:' (Type), the dropdown menu is set to 'Benutzerdefinierte Endungen' (Custom Extensions). Below this, the 'Erweiterungen:' (Extensions) field contains a list of file extensions: 'exe' and 'bat'.

Optionen für die Computer-Scan-Aufgabe - Hinzufügen von benutzerdefinierten Endungen

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierte Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, Archive zu scannen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

**Wichtig**

Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten. Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
 - **Archivgröße begrenzen auf (MB).** Sie können die maximale Größe der Archive angeben, die gescannt werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
 - **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.
- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

**Wichtig**

Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
 - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
 - **Registrierung scannen.** Wählen Sie diese Option, um die Registrierungsschlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und

Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.

- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach **Rootkits** und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, um nach **Keylogger**-Software zu suchen.
- **Netzwerkfreigaben scannen.** Mit dieser Option werden bereitgestellte Netzwerklaufwerke überprüft.

Für Schnell-Scans ist diese Option standardmäßig deaktiviert. Für vollständige Scans ist diese Option standardmäßig aktiviert. Bei benutzerdefinierte Scans ist die Option the **Netzwerkfreigaben scannen** automatisch aktiviert, wenn Sie als Sicherheitsstufe **aggressiv/normal** wählen. Falls Sie die Sicherheitsstufe **tolerant** wählen, wird die Option **Netzwerkfreigabe scannen** automatisch deaktiviert.

- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf dem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Auf potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser

installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

- **Wechseldatenträger scannen.** Wählen Sie diese Option, um Wechseldatenträger zu scannen, die mit dem Computer verbunden sind.
- **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
 - **Wenn eine infizierte Datei gefunden wird.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI). Der Bitdefender-Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

Wenn eine infizierte Datei gefunden wird, versucht der Bitdefender-Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.



Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Wenn eine verdächtige Datei gefunden wird.** Dateien werden durch heuristische Analysen und andere Bitdefender-Technologien als verdächtig erkannt. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden). Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden. Dateien in Quarantäne werden

zu Analysezwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Wenn ein Rootkit gefunden wurde.** Rootkits sind spezielle Software-Werkzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie. Wählen Sie aus den entsprechenden Menüs die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll. Folgende Aktionen stehen zur Verfügung:

Desinfizieren

Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Dateien in Quarantäne verschieben

Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die [Quarantäne](#)-Seite in der Konsole verwalten.

Löschen

Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Ignorieren

Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

- Gehen Sie zum Reiter **Ziel**, um die Speicherorte zu konfigurieren, die auf den Computern gescannt werden sollen.

Im Bereich **Scan-Ziel** können Sie eine neue Datei oder einen neuen Ordner hinzufügen, die/der gescannt werden soll:

- a. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.
- b. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.
 - Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen. Um einen bestimmten Order im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.
 - Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist. Weitere Informationen zu den Systemvariablen finden Sie unter „[Systemvariablen](#)“ (S. 546).

- c. Klicken Sie auf den entsprechenden **+** **Hinzufügen**-Link.

Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an. Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende **×** **Löschen**-Schaltfläche.

Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.

Klicken Sie auf den Bereich **Ausschlüsse**, wenn Sie bestimmte Ziele ausschließen möchten.

▼ **Ausschlüsse**

Verwenden Sie die unter **Richtlinie > Malware-Schutz > Ausschlüsse** definierten Ausschlüsse.

Für diesen Scan benutzerdefinierte Ausschlüsse definieren

Datei	Bestimmte Pfade	+
Ausschlussart	Zu scannende Dateien und Ordner	Aktion

Speichern **Abbrechen**

Computer-Scan-Aufgabe - Definieren von Ausschlüssen

Sie können entweder die per Richtlinie definierten Ausschlüsse verwenden oder für die aktuelle Scan-Aufgabe bestimmte Ausschlüsse definieren. Weitere Informationen finden Sie unter „[Ausschlüsse](#)“ (S. 301).

7. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).



Beachten Sie

Zum Planen von Scan-Aufgaben öffnen Sie die Seite **Richtlinien**, wählen Sie die dem entsprechenden Computer zugewiesene Richtlinie aus und fügen Sie im Bereich **Malware-Schutz > Bei Bedarf** eine Scan-Aufgabe hinzu. Weitere Informationen finden Sie unter „[Bedarf-Scan](#)“ (S. 279).

Patch-Aufgaben

Es wird empfohlen, regelmäßig zu prüfen, ob Softwareupdates zur Verfügung stehen und diese so schnell wie möglich einzuspielen. Mit GravityZone lässt sich dieser Vorgang durch Sicherheitsrichtlinien automatisieren. Wenn Sie die Software auf bestimmten Endpunkten jedoch sofort aktualisieren möchten, führen Sie die folgenden Aufgaben in dieser Reihenfolge durch:


1. [Patch-Scan](#)
2. [Patch-Installation](#)

Vorbereitende Maßnahmen

- Der Sicherheitsagent mit dem Patch-Verwaltungs-Modul wurde auf den Zielendpunkten installiert.
- Damit die Scan- und Installationsaufgaben erfolgreich durchgeführt werden können, müssen auf den Windows-Endpunkten die folgenden Bedingungen erfüllt sein:
 - Das **DigiCert Assured ID Root CA**-Zertifikat ist unter **Vertrauenswürdige Stammzertifizierungsstellen** gespeichert.
 - **Vorübergehende Zertifizierungsstellen** umfasst das **DigiCert SHA2 Assured ID Code Signing CA**-Zertifikat.
 - Auf den Endpunkten sind die Patches für Windows 7 und Windows Server 2008 R2 installiert, die in diesem Microsoft-Artikel erwähnt sind: [Microsoft Security Advisory 3033929](#)

Patch-Scan

Endpunkte mit veralteter Software sind anfällig für Angriffe. Es empfiehlt sich daher, die auf Ihren Endpunkten installierte Software regelmäßig zu überprüfen und Updates so schnell wie möglich einzuspielen. Gehen Sie folgendermaßen vor, um Ihre Endpunkte auf fehlende Patches zu überprüfen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Zielendpunkte aus.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Patch-Scan** aus. Ein Bestätigungsfenster wird angezeigt.
6. Klicken Sie zur Bestätigung der Scan-Aufgabe auf **Ja**.

Nach Abschluss der Aufgabe fügt GravityZone alle von Ihrer Software benötigten Patches dem Patch-Inventar hinzu. Weitere Informationen finden Sie unter [„Patch-Inventar“ \(S. 205\)](#).

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“ \(S. 214\)](#).




Beachten Sie


Um einen Zeitplan für die Patch-Scans festzulegen, bearbeiten Sie die den Zielendpunkten zugewiesenen Richtlinien und konfigurieren Sie die Einstellungen im Bereich **Patch-Verwaltung**. Weitere Informationen finden Sie unter „[Patch-Verwaltung](#)“ (S. 351).

Patch-Installation

Gehen Sie folgendermaßen vor, um einen oder mehrere Patches auf den Zielendpunkten zu installieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Patch-Installation** aus.

Ein Konfigurationsfenster wird sich öffnen. Hier können Sie alle Patches einsehen, die auf den Zielendpunkten fehlen.

5. Nutzen Sie bei Bedarf die Sortierungs- und Filtermöglichkeiten am oberen Rand der Tabelle, um nach bestimmten Patches zu suchen.
6. Klicken Sie auf die Schaltfläche  **Spalten** oben rechts im Fenster, um nur relevante Informationen anzuzeigen.
7. Wählen Sie die Patches aus, die Sie installieren möchten.

Es gibt Patches, die von anderen Patches abhängen. Ist dies der Fall werden Sie automatisch gemeinsam mit dem entsprechenden Patch ausgewählt.

Mit einem Klick auf die Ziffern von **CVEs** oder **Produkten** wird links ein neuer Bereich angezeigt. In diesem Bereich finden Sie zusätzliche Informationen, so zum Beispiel die CVEs, die durch das Patch behoben werden und die Produkte, auf die das Patch angewendet wird. Klicken Sie auf **Schließen**, wenn Sie alles gelesen haben, um den Bereich wieder zu schließen.

8. Wählen Sie zum Neustart von Endpunkten unmittelbar nach der Patch-Installation die Option **Falls nötig, Endpunkte nach Installation des Patches neu starten**, wenn ein Systemstart erforderlich ist. Bitte bedenken Sie, dass diese Aktion Benutzer bei der Arbeit stören könnte.
9. Klicken Sie auf **Installieren**.

Die Installationsaufgabe wird gemeinsam mit allen Unteraufgaben für jeden Zielendpunkt erstellt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Beachten Sie

- Um einen Zeitplan für die Patch-Installation festzulegen, bearbeiten Sie die den Zielendpunkten zugewiesenen Richtlinien und konfigurieren Sie die Einstellungen im Bereich **Patch-Verwaltung**. Weitere Informationen finden Sie unter „[Patch-Verwaltung](#)“ (S. 351).
- Sie können für Sie interessante Patches zudem über die Seite **Patch-Inventar** installieren. Wählen Sie dazu das Patch aus der Liste aus, klicken Sie am oberen Rand der Tabelle auf **Installieren** und konfigurieren Sie die Installationsdetails. Weitere Informationen finden Sie unter „[Installieren von Patches](#)“ (S. 209).
- Nach Installation eines Patches empfiehlt es sich, eine **Patch-Scan**-Aufgabe an die Zielendpunkte zu übermitteln. Durch diese Aktion werden die in GravityZone gespeicherten Patch-Informationen für Ihre verwalteten Netzwerke aktualisiert.

Sie haben folgende Optionen zur Deinstallation von Patches:

- Per Fernzugriff durch Übermittlung einer [Aufgabe zur Patch-Deinstallation](#) über GravityZone.
- Lokal auf dem Endpunkt. Dazu müssen Sie sich als Administrator am Endpunkt anmelden und das Deinstallationsprogramm manuell ausführen.

Exchange-Scan

Sie können die Datenbank eines Exchange-Servers aus der Ferne scannen, indem Sie eine **Exchange-Scan**-Aufgabe ausführen.

Damit der Scan einer Exchange-Datenbank durchgeführt werden kann, müssen Sie Bedarf-Scans aktivieren, indem Sie die Zugangsdaten eines Exchange-Administrators eingeben. Weitere Informationen finden Sie unter „[Scannen des Exchange-Informationsspeichers](#)“ (S. 377).

So scannen Sie eine Exchange-Server-Datenbank:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe aus, die den gewünschten Exchange-Server enthält. Sie finden den Server dann im rechten Fenster.



Beachten Sie

Sie können auch Filter verwenden, um den gewünschten Server schneller zu finden:

- Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Verwaltet (Exchange-Server)** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.
- Geben Sie den Hostnamen oder die IP-Adresse des Servers in die Felder der entsprechenden Spaltenüberschrift ein.

4. Markieren Sie das Kästchen des Exchange-Servers, dessen Datenbank Sie scannen möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Exchange-Scan**. Ein Konfigurationsfenster wird sich öffnen.
6. Konfigurieren Sie die Scan-Optionen:

- **Allgemein.** Geben Sie einen aussagekräftigen Namen für die Aufgabe ein.

Bei großen Datenbanken kann der Scan lange dauern und die Serverleistung beeinträchtigen. Markieren Sie in solchen Fällen das Kästchen **Scan stoppen, wenn er länger dauert als** und wählen Sie einen beliebigen Zeitraum aus den entsprechenden Menüs

- **Ziel.** Hier können Sie Container und Objekte auswählen, die gescannt werden sollen. Sie können Postfächer, öffentliche Ordner oder beides scannen lassen. Außer E-Mails können Sie auch andere Objekte wie **Kontakte, Aufgaben, Termine** und **Mail-Objekte** scannen lassen. Außerdem können Sie den Scan wie folgt einschränken:

- Nur ungelesene E-Mails
- Nur Objekte mit Anhängen
- Nur neue Objekte, die in einem bestimmten Zeitraum empfangen wurden

So können Sie zum Beispiel nur E-Mails in Benutzer-Postfächern scannen lassen, die in den letzten sieben Tagen empfangen wurden.

Markieren Sie das Kästchen **Ausschlüsse**, wenn Sie Scan-Ausnahmen definieren möchten. So erstellen Sie mithilfe der Felder in der Tabellenüberschrift eine Ausnahme:

- a. Wählen Sie den Repository-Typ aus dem Menü.
- b. Geben Sie je nach Repository-Typ das auszuschließende Objekt an:

Repository-Typ	Objektformat
Postfach	E-Mail-Adresse


Repository-Typ	Objektformat
Öffentlicher Ordner	Ordnerpfad, von Root ausgehend
Datenbank	Die Datenbankidentität


Beachten Sie

Mit dem folgenden Exchange-Shell-Befehl können Sie die Datenbankidentität abrufen:

```
Get-MailboxDatabase | fl name,identity
```

Sie können nicht mehr als ein Objekt gleichzeitig eingeben. Wenn Sie mehrere Objekte desselben Typs haben, müssen Sie für jedes einzelne Objekt eine eigene Regel definieren.

- c. Klicken Sie am oberen Rand der Tabelle auf die Schaltfläche  **Hinzufügen**, um die Ausnahme zu speichern und der Liste hinzuzufügen.

Um eine Ausnahmenregel aus der Liste zu löschen, klicken Sie auf die entsprechende  **Löschen**-Schaltfläche.

- **Optionen.** Hier können Sie die Scan-Optionen für E-Mails einstellen, die zu einer Regel passen:
 - **Gescannte Dateitypen.** Mit dieser Option legen Sie fest, welche Dateitypen gescannt werden. Sie können einstellen, dass alle Dateien gescannt werden (unabhängig von der Dateiendung), nur Anwendungsdateien oder nur bestimmte Dateiendungen, die Sie für gefährlich halten. Das Scannen aller Dateien bietet den besten Schutz, nur Anwendungsdateien zu scannen ist schneller.

Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 545).

Wenn Sie nur Dateien mit bestimmten Endungen scannen möchten, haben Sie zwei Möglichkeiten:

- **Benutzerdefinierte Endungen;** geben Sie hier nur die Endungen der Dateitypen ein, die gescannt werden sollen.
- **Alle Dateien außer bestimmten Endungen;** hierbei geben sie nur die Dateiendungen ein, die nicht gescannt werden sollen.
- **Maximalgröße für Anhang/Nachrichteninhalt (in MB).** Markieren Sie dieses Kästchen und geben Sie einen Wert in das entsprechende Feld

ein, um die Maximalgröße für angehängte Dateien oder Nachrichteninhalte festzulegen, bis zu der gescannt werden soll.

- **Maximale Archivtiefe (Ebenen).** Markieren Sie dieses Kästchen und wählen Sie die maximale Archivtiefe im entsprechenden Feld. Je geringer dieser Wert, desto höher die Leistung und geringer die Sicherheit.
- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Markieren Sie dieses Kästchen, um nach potenziell bösartigen oder unerwünschten Anwendungen zu scannen, z. B. Adware, die sich ohne Zustimmung des Benutzers auf dem System installiert, das Verhalten anderer Software beeinflusst oder die Systemleistung einschränkt.
- **Aktionen.** Sie können für den Sicherheitsagenten abhängig von der Erkennungsart verschiedene automatische Aktionen für Dateien festlegen.

Über die Erkennungsart werden Dateien in drei Kategorien unterteilt:

- **Infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI).
- **Verdächtige Dateien.** Diese Dateien werden durch heuristische Analyse und andere Bitdefender-Technologien als verdächtig eingestuft. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden).
- **Unscanbare Dateien.** Diese Dateien können nicht gescannt werden. So können zum Beispiel passwortgeschützte, verschlüsselte oder überkomprimierte Dateien nicht gescannt werden.

Für jeden Erkennungstyp gibt es eine Standard- oder Hauptaktion und eine alternative Aktion für den Fall, dass die Hauptaktion fehlschlägt. Es wird nicht empfohlen, aber wenn Sie möchten, können Sie diese Aktionen über die entsprechenden Menüs ändern. Wählen Sie die Aktion, die ausgeführt werden soll:

- **Desinfizieren.** Entfernt den schädlichen Code aus infizierten Dateien und rekonstruiert die Originaldatei. Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
- **E-Mail ablehnen/löschen.** Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen

anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

- **Datei löschen.** Entfernt problematische Anhänge ohne Warnung. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei ersetzen.** Entfernt problematische Dateien und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert.
- **Datei in die Quarantäne verschieben.** verschiebt erkannte Dateien in den Quarantäneordner und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. In die Quarantäne verschobene Dateien können Sie auf der Seite **Quarantäne** verwalten.



Beachten Sie

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist. Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

- **Keine Aktion durchführen.** Wenn problematische Dateien gefunden werden, wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen. Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.
 - Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden.**
7. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.
 8. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“ \(S. 214\)](#).

Installieren

Um Ihre Computer zu schützen, müssen Sie auf jedem von ihnen den Bitdefender-Sicherheitsagenten installieren.



Wichtig

In isolierten Netzwerken, die keine direkte Verbindung zur GravityZone-Appliance haben, können Sie den Sicherheitsagenten mit der [Relais-Rolle](#) installieren. In diesem Fall läuft die Kommunikation zwischen der GravityZone-Appliance und den anderen Sicherheitsagenten über den Relais-Agenten, der auch als lokaler Update-Server für die Sicherheitsagenten des isolierten Netzwerks fungiert.

Sobald Sie einen Relais-Agenten installiert haben, findet dieser automatisch ungeschützte Computer im selben Netzwerk.



Beachten Sie

- Der Computer, auf dem Sie den Relais-Agenten installieren, sollte immer eingeschaltet sein.
- Wenn in dem Netzwerk kein Relais-Agent installiert ist, kann die Erkennung ungeschützter Computer manuell durchgeführt werden. Dazu muss eine **Netzwerkerkennung**-Aufgabe an einen geschützten Endpunkt geschickt werden.

Die Bitdefender-Sicherheitssoftware kann per Fernzugriff über das Control Center auf Computern installiert werden.

Die Remote-Installation erfolgt im Hintergrund, ohne dass der Benutzer dies bemerkt.



Warnung

Vor der Installation sollten Sie bereits installierte Malware-Schutz- und Firewall-Software deinstallieren. Wenn die Bitdefender-Sicherheitssoftware über bestehende Sicherheitssoftware installiert wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen. Windows Defender und die Windows-Firewall werden beim Start der Installation automatisch deaktiviert.

Falls Sie den Sicherheitsagenten auf einem Computer mit Bitdefender Antivirus for Mac 5.X installieren möchten, müssen Sie letzteren zunächst deinstallieren. Sie finden eine Anleitung in diesem [Artikel in der Wissensdatenbank](#).

Wenn Sie den Agenten über ein Linux-Relais installieren, müssen die folgenden Voraussetzungen erfüllt sein:

- Auf dem Relais-Endpoint muss das Samba-Paket (`smbclient`) mindestens in der Version 4.1.0 sowie der `net-Binary/Befehl` installiert sein, um Windows-Agenten installieren zu können.

**Beachten Sie**

Der `net`-Binary/Befehl wird üblicherweise mit den Paketen `samba-client` und `/` oder `samba-common` ausgeliefert. Bei einigen Linux-Distributionen (z. B. CentOS 7.4) wird der `net`-Befehl nur bei der Installation der kompletten Samba-Suite (Common + Client + Server) installiert. Stellen Sie sicher, dass auf Ihrem Relais-Endpunkt der `net`-Befehl verfügbar ist.


- Auf den gewünschten Windows-Endpunkten müssen Administratorfreigabe und Netzwerkfreigabe aktiviert sein.
- Auf den gewünschten Linus- und Mac-Endpunkten muss SSH aktiviert und die Firewall deaktiviert sein.

So führen Sie eine Ferninstallationsaufgabe aus:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
4. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

**Beachten Sie**

Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Endpunkte anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

5. Wählen Sie die Entitäten (Endpunkte oder Gruppen von Endpunkten) aus, auf denen Sie den Schutz installieren möchten.
6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Installieren**.

Der Assistent **Client installieren** wird angezeigt.

Benutzer	Passwort	Beschreibung	Aktion
<input type="checkbox"/> admin	*****		<input checked="" type="checkbox"/>

Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

7. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:

- **Jetzt** - hiermit startet die Installation sofort.
- **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.



Beachten Sie

Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

8. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
9. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.

**Wichtig**

Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in [diesem Artikel](#).

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

- a. Geben Sie im entsprechenden Feld in der Spaltenüberschrift den Benutzernamen und das Passwort eines Administratorkontos ein.

Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

Bei der Eingabe des Namens eines Nutzerkontos Windows-Konvention verwenden:

- Für Active Directory-Maschinen wird folgende Syntax verwendet: `username@domain.com` und `Domäne\Benutzername`. Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).
- Bei Arbeitsgruppen-Maschinen genügt die Eingabe des Benutzernamens ohne Angabe des Namens der Arbeitsgruppe.

Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

- b. Klicken Sie auf den Button **+Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.

**Beachten Sie**

Die angegebenen Zugangsdaten werden automatisch im [Zugangsdaten-Manager](#) gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben werden müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren.

**Wichtig**

Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

10. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.



Beachten Sie

Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation des Sicherheitsagenten auf Endpunkten nicht ausgelassen werden.

11. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.

- **GravityZone-Appliance**, wenn die Endpunkte eine direkte Verbindung zur GravityZone-Appliance herstellen.

In diesem Fall können Sie auch Folgendes definieren:

- Einen benutzerdefinierten Kommunikationsserver; geben Sie dazu, falls erforderlich, die entsprechende IP-Adresse oder den Hostnamen ein.
- Proxy-Einstellungen, wenn die Endpunkte über einen Proxy-Server mit der GravityZone-Appliance kommunizieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in die entsprechenden Felder ein.

- **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.



Wichtig

Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.

Installer			
Installer:			Endpoint-Security-Relais
Name	IP	Benutzerdefinierter Server...	Bezeichnung
MASTER-PC	10.10.127.162		N/A

12. Im Bereich **Zusätzliche Ziele** können Sie den Client auf bestimmten Maschinen in Ihrem Netzwerk installieren, die nicht im Netzwerkinventar angezeigt werden. Vergrößern Sie den Bereich und geben Sie die IP-Adressen oder die Hostnamen dieser Maschinen, durch Kommas getrennt, in das entsprechende Feld ein. Sie können so viele IP-Adressen wie nötig hinzufügen.
13. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.
14. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Bearbeitung von Installationspaketen finden Sie in der GravityZone-Installationsanleitung.

Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.

15. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

Wichtig

Wenn Sie VMware Horizon View Persona Management verwenden, wird empfohlen, die Active Directory-Gruppenrichtlinien so zu konfigurieren, dass die folgenden Bitdefender-Prozesse ausgeschlossen werden (ohne den vollständigen Pfad):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Diese Ausschlüsse müssen angewendet werden, solange der Sicherheitsagent auf dem Endpunkt läuft. Weitere Einzelheiten finden Sie auf dieser [Seite der VMware-Horizon-Dokumentation](#).


Client-Upgrade durchführen

Diese Aufgabe ist nur dann verfügbar, wenn der Endpoint Security-Agent installiert und im Netzwerk erkannt wurde. Bitdefender empfiehlt ein Upgrade von Endpoint Security auf das neue **Bitdefender Endpoint Security Tools**, um Endpunktschutz der neuesten Generation sicherzustellen.

Über einen **Upgrade**-Statusbericht lässt sich bequem feststellen, welche Clients noch kein Upgrade erhalten haben. Einzelheiten zum Erstellen von Berichten finden Sie unter „**Berichte erstellen**“ (S. 459).

Client Deinstallieren

So entfernen Sie die Bitdefender-Sicherheitssoftware per Fernzugriff:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client deinstallieren**.
6. Ein Konfigurationsfenster wird angezeigt, in dem Sie die folgenden Einstellungen vornehmen können:
 - Wenn Sie möchten, können Sie die Quarantäne-Objekte auf der Client-Maschine belassen.
 - Bei mit vShield integrierten Umgebungen müssen Sie die erforderlichen Zugangsdaten für jede Maschine auswählen, da die Deinstallation sonst fehlschlägt. Wählen Sie **Zugangsdaten für die vShield-Integration verwenden** und markieren Sie dann alle nötigen Zugangsdaten aus der unten angezeigten Zugangsdaten-Manager-Tabelle.
7. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „**Aufgaben anzeigen und verwalten**“ (S. 214).



Beachten Sie


Wenn Sie den Schutz erneut installieren möchten, müssen Sie den Computer zuerst neu starten.

Client aktualisieren

Überprüfen Sie den Status verwalteter Computer in regelmäßigen Abständen. Wenn Ihnen ein Computer mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um die Seite **Informationen** anzuzeigen. Weitere Informationen finden Sie unter „**Sicherheitsstatus**“ (S. 52).

Veraltete Clients oder Sicherheitsinhalten stellen Sicherheitsprobleme dar. In diesen Fälle sollten Sie ein Update auf dem entsprechenden Computer durchführen. Diese Aufgabe kann lokal vom Computer aus oder per Fernzugriff von der Control Center aus durchgeführt werden.

So können Sie den Client und die Sicherheitsinhalte auf verwalteten Computern per Fernzugriff aktualisieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer ,auf denen Sie ein Client-Update durchführen möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Update**. Ein Konfigurationsfenster wird sich öffnen.
6. Sie können nur das Produkt, nur die Sicherheitsinhalte oder beides aktualisieren.
7. Bei Linux-Betriebssystemen und mit vShield integrierten Maschinen müssen die nötigen Zugangsdaten ebenfalls ausgewählt werden. Markieren Sie **Zugangsdaten für Linux und die vShield-Integration verwenden** und wählen Sie dann die nötigen Zugangsdaten aus der unten angezeigten Zugangsdaten-Manager-Tabelle.
8. Klicken Sie auf **Update**, um die Aufgabe auszuführen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „**Aufgaben anzeigen und verwalten**“ (S. 214).

Client neu konfigurieren

Die Module, Rollen und Scan-Modi des Sicherheitsagenten sind zunächst im Installationspaket konfiguriert. Nach der Installation des Sicherheitsagenten in Ihrem Netzwerk können Sie die anfänglichen Einstellungen jederzeit ändern, indem Sie per Fernzugriff einer Aufgabe **Client neu konfigurieren** an die gewünschten verwalteten Endpunkte senden.

Warnung


Bitte beachten Sie, dass die Aufgabe **Client neu konfigurieren** alle Installationseinstellungen überschreibt. Keine der ursprünglich Einstellungen wird beibehalten. Achten Sie bei der Verwendung dieser Aufgabe darauf, alle Installationseinstellungen für die gewünschten Endpunkte neu zu konfigurieren.

Beachten Sie

Die Aufgabe **Client neu konfigurieren** entfernt alle nicht unterstützten Module von bestehenden Installationen auf veralteten Windows-Systemen.

Sie können die Installationseinstellungen über den Bereich **Netzwerk** oder über den Bericht **Status der Endpunktmodule** ändern.

So ändern Sie die Installationseinstellungen für einen oder mehrere Computer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer, bei denen Sie die Installationseinstellungen ändern möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client neu konfigurieren**.
6. Wählen Sie eine der folgenden Aktionen:
 - **Hinzufügen**. Neue Module zu den bestehenden hinzufügen.
 - **Entfernen**. Bestimmte Module entfernen.
 - **Abgleichsliste**. Gleichen Sie die installierten Module mit Ihrer Auswahl ab.
7. Wählen Sie die Module und Rollen, die Sie auf den Zielcomputern hinzufügen oder entfernen möchten.



Warnung

Es können nur unterstützte Module installiert werden. Die Firewall, z. B., kann nur auf den unterstützten Windows-Arbeitsplatzrechnern installiert werden.

Weitere Informationen hierzu finden Sie unter [Verfügbarkeit der GravityZone-Sicherheitsebenen](#).

8. Wählen Sie **Konkurrenzprodukte entfernen, falls erforderlich** um zu gewährleisten, dass die gewählten Module nicht in Konflikt mit anderen evtl. auf den Endpunkten installierten Sicherheitslösungen in Konflikt geraten.
9. Wählen Sie den gewünschten Scan-Modus:
 - **Automatisch.** Der Sicherheitsagent erkennt automatisch, welche Scan-Engines für die Ressourcen des Endpunkts am besten geeignet sind.
 - **Benutzerdef.** Sie wählen die Scan-Engines, die Sie nutzen möchten.Weitere Informationen zu den verfügbaren Optionen erhalten Sie im Abschnitt „Installationspakete erstellen“ der Installationsanleitung.



Beachten Sie

Dieser Bereich steht nur mit der Option **Listenabgleich** zur Verfügung.

10. Stellen Sie im Bereich **Planer** ein, wann die Aufgabe ausgeführt werden soll:
 - **Jetzt** - hiermit startet die Aufgabe sofort.
 - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Aufgabe fest.Wählen Sie einfach das gewünschte Intervall (stündlich, täglich oder wöchentlich).
11. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“ \(S. 214\)](#).

Client reparieren

Verwenden Sie die Aufgabe Client reparieren zur ersten Fehlerbehebung für verschiedenste Endpunktproblemen. Mit dieser Aufgabe wird das neueste Installationspaket auf den Zielpunkt heruntergeladen und anschließend der Agent neu installiert.

i Beachten Sie

- The modules currently configured on the agent will not be changed.
- Die Reparaturaufgabe setzt den Sicherheitsagenten auf die Version zurück, die auf der Seite **Konfiguration > Update > Komponenten** angegeben ist.

So übermitteln Sie die Aufgabe Client reparieren an einen Client:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer, auf denen Sie eine Client-Reparatur durchführen möchten.
5. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Client reparieren**. Ein Bestätigungsfenster wird angezeigt.
6. Markieren Sie das Kästchen **Ich habe das verstanden und stimme dem zu** und klicken Sie auf die Schaltfläche **Speichern**, um die Aufgabe auszuführen.

i Beachten Sie

Um die Reparaturaufgabe abzuschließen, muss der Client evtl. neu gestartet werden.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „**Aufgaben anzeigen und verwalten**“ (S. 214).


Computer neu starten

Sie können verwaltete Computer aus der Ferne neu starten, wenn Sie möchten.

i Beachten Sie

Bevor Sie einzelne Computer neu starten, sollten Sie einen Blick auf die Seite **Netzwerk > Aufgaben** werfen. Zuvor erstellte Aufgaben könnten zurzeit noch auf den ausgewählten Computern laufen.


1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.

3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der Computer, die Sie neu starten möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Computer neu starten**.
6. Wählen Sie den Zeitpunkt des Neustarts:
 - Wählen Sie **Jetzt neu starten**, um die Computer sofort neu zu starten.
 - Wählen Sie **Neustart am**, und nutzen Sie die Eingabefelder weiter unten, um den Neustart für einen bestimmten Zeitpunkt zu planen.
7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.
Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Netzwerkerkennung


Die Netzwerkerkennung wird automatisch von Sicherheitsagenten mit **Relais-Rolle** durchgeführt. Wenn Sie in Ihrem Netzwerk keinen Relais-Agenten installiert haben, müssen Sie manuell eine Netzwerkerkennungsaufgabe von einem geschützten Endpunkt aus senden.

So führen Sie eine Netzwerkerkennungsaufgabe in Ihrem Netzwerk durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen des Computers, über den Sie eine Netzwerkerkennung durchführen möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Netzwerkerkennung**.
6. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.
Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Anwendungserkennung

So können Sie die Anwendungen in Ihrem Netzwerk ermitteln:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Computer aus, auf denen die Anwendungen ermittelt werden sollen.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Anwendungserkennung** aus.



Beachten Sie

Auf den ausgewählten Computern muss Bitdefender Endpoint Security Tools mit Anwendungssteuerung installiert und aktiviert sein. Andernfalls wird die Aufgabe ausgegraut. Wenn eine ausgewählte Gruppe sowohl gültige als auch ungültige Ziele enthält, wird die Aufgabe nur an die gültigen Endpunkte übermittelt.

6. Klicken Sie zum Fortsetzen des Vorgangs im Bestätigungsfenster auf **Ja**.

Die ermittelten Anwendungen und Prozesse werden auf der Seite **Netzwerk- > Anwendungsbestand** angezeigt. Weitere Informationen finden Sie unter „[Anwendungsbestand](#)“ (S. 199).



Beachten Sie

Die Aufgabe **Anwendungserkennung** kann je nach Anzahl der installierten Anwendungen einige Zeit in Anspruch nehmen. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Security Server aktualisieren

Installierte Security Server können auch unter **Computer und virtuelle Maschinen** im Ordner **Benutzerdefinierte Gruppen** angezeigt und verwaltet werden.

Wenn ein Security Server veraltet ist, können Sie eine Update-Aufgabe an ihn senden:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).

3. Wählen Sie die Gruppe, in der der Security Server installiert ist.

Den Security Server finden Sie leicht über das **Filter**menü. Gehen Sie dazu wie folgt vor:

- Gehen Sie zum Reiter **Sicherheit** und wählen Sie nur **Security Servers** aus.
- Gehen Sie zum Reiter **Tiefe** und wählen Sie **Alle Objekte rekursiv**.

4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Security Server aktualisieren**.

5. Sie müssen die Aktion bestätigen. Klicken Sie auf **Ja**, um die Aufgabe zu erstellen.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).



Wichtig

Diese Methode wird für Updates von Security Server for NSX empfohlen, da andernfalls die auf der Appliance gespeicherte Quarantäne verloren gehen würde.

Benutzerdefiniertes Tool injizieren

Gehen Sie folgendermaßen vor, um Tools in Ziel-Gastbetriebssystemen zu injizieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Kästchen für die Zielendpunkte aus.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Benutzerdefiniertes Tool injizieren**. Ein Konfigurationsfenster wird geöffnet.
6. Wählen Sie aus dem Klappmenü alle zu injizierenden Tools aus. Für jedes Tool wird ein reduzierbarer Bereich mit den entsprechenden Einstellungen angezeigt. Diese Tools wurden zuvor in GravityZone hochgeladen. Wenn das gesuchte Tool in der Liste nicht aufgeführt ist, rufen Sie das **Tool-Verwaltungszentrum** auf

und fügen Sie es von dort aus hinzu. Weitere Informationen finden Sie unter „Benutzerdefiniert Tool-Injektion mit HVI“ (S. 511).

7. Gehen Sie für jedes im Fenster angezeigt Tool folgendermaßen vor:
 - a. Klicken Sie auf den Namen des Tools, um den entsprechenden Bereich anzuzeigen oder zu verbergen.
 - b. Geben Sie die Befehlszeile des Tools gemeinsam mit allen benötigten Eingabeparametern ein, so wie Sie es auch in der Eingabeaufforderung bzw. im Terminal tun würden. Zum Beispiel:

```
bash script.sh <param1> <param2>
```


Für die BD-Bereinigungstools können Sie aus den beiden Klappmenüs nur die Bereinigungsaktion sowie die Ersatzaktion zur Bereinigung auswählen.

- c. Verweisen Sie auf den Speicherort, von dem der Security Server die Protokolle abrufen soll:
 - **stdout**. Markieren Sie das Kästchen, um die Protokolle über den Standard-Ausgangsübertragungskanal abzurufen.
 - **Ausgabedatei**. Markieren Sie dieses Kästchen, um auf dem Endpunkt gespeicherte Protokolldateien abzurufen. In diesem Fall müssen Sie den Pfad eingeben, über den der Security Server die Datei finden kann. Sie können sowohl absolute Pfade als auch Systemvariablen eingeben.
Hier eine weitere Option: **Protokolldateien nach der Übermittlung vom Gast löschen**. Wählen Sie diese Option, wenn die Dateien auf dem Endpunkt nicht mehr benötigt werden.
8. Wenn Sie die Protokolldateien vom Security Server zu einem anderen Speicherort verschieben möchten, müssen Sie den Pfad zum Zielspeicherort und die Anmeldeinformationen für die Authentifizierung angeben.
9. Gelegentlich braucht das Tool unter Umständen länger als erwartet, um den Auftrag abzuschließen, oder reagiert nicht mehr. Um in diesen Fällen Abstürze zu verhindern, können Sie im Bereich **Sicherheitskonfiguration** festlegen, nach wie vielen Stunden der Security Server den Tool-Prozess automatisch beenden soll.
10. Klicken Sie auf **Speichern**.

Auf der Seite **Aufgaben** können Sie den Aufgabenstatus einsehen. Weitere Details finden Sie zudem im **HVI-Drittanbieter-Injektionsstatus-Bericht**.

6.2.6. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte auf verwalteten Computern erstellen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
Optional können Sie den Inhalt der ausgewählten Gruppe nur nach verwalteten Computern filtern.
4. Markieren Sie die Kästchen der Computer, die im Bericht enthalten sein sollen.
5. Klicken Sie auf die Schaltfläche  **Bericht** am oberen Rand der Tabelle, und wählen Sie den Berichtstyp aus dem Menü.

Weitere Informationen finden Sie unter „[Berichte zu Computern und virtuellen Maschinen](#)“ (S. 439).

6. Konfigurieren Sie die Berichtsoptionen. Weitere Informationen finden Sie unter „[Berichte erstellen](#)“ (S. 459).
7. Klicken Sie auf **Generieren**. Der Bericht wird sofort angezeigt.
Es dauert unterschiedlich lange, bis Berichte erstellt sind, je nach Anzahl der ausgewählten Computer.

6.2.7. Richtlinien zuweisen

Über **Richtlinien** können Sie Sicherheitseinstellungen auf Computern verwalten.

Auf der Seite **Netzwerk** können Sie Richtlinien für jeden Computer bzw. Gruppe von Computern anzeigen, ändern und zuweisen.



Beachten Sie


Sicherheitseinstellungen stehen nur für verwaltete Computer zur Verfügung. Um Sicherheitseinstellungen leichter überblicken und verwalten zu können, können Sie das Netzwerkinventar auch nach verwalteten Computern **filtern**.

So zeigen Sie an, welche Richtlinie einem bestimmten Computer zugewiesen wurde:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
4. Klicken Sie auf den Namen des verwalteten Computers, der Sie interessiert. Es öffnet sich ein Informationsfenster.
5. Klicken Sie im Reiter **Allgemein** des Bereichs **Richtlinie** auf den Namen der aktuellen Richtlinie, um ihre Einstellungen anzuzeigen.
6. Sie können die Sicherheitseinstellungen nach Bedarf ändern, sofern der Richtlinienersteller Änderungen an dieser Richtlinie durch andere Benutzer erlaubt hat. Bitte beachten Sie, dass sich Ihre Änderungen auf alle Computer auswirken, denen diese Richtlinie zugewiesen wurde.

Weitere Informationen zu Computer-Richtlinieneinstellungen finden Sie unter [„Richtlinien für Computer und virtuelle Maschinen“](#) (S. 244).


So weisen Sie einem Computer oder einer Gruppe eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen des gewünschten Computers bzw. der gewünschten Gruppe. Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
5. Klicken Sie auf die Schaltfläche  **Richtlinie zuweisen** am oberen Ende der Tabelle.
6. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor. Weitere Informationen finden Sie unter [„Richtlinien zuweisen“](#) (S. 231).

Der Wiederherstellungsmanager für verschlüsselte Laufwerke

Wenn Endpunkt-Benutzer ihr Verschlüsselungspasswort vergessen und somit nicht mehr auf verschlüsselte Laufwerke ihres Computers zugreifen können, können Sie ihnen mit Wiederherstellungsschlüsseln von der Seite **Netzwerk** helfen.

So rufen Sie einen Wiederherstellungsschlüssel ab:

1. Gehen Sie zur Seite **Netzwerk**.
2. Klicken Sie in der Symbolleiste des linken Fensters auf die Schaltfläche  **Wiederherstellungsmanager**. Ein neues Fenster wird angezeigt.
3. Geben Sie im Bereich **Bezeichner** des Fensters die folgenden Daten ein:

- a. Die Wiederherstellungsschlüssel-ID des verschlüsselten Laufwerks. Die Wiederherstellungsschlüssel-ID ist eine Folge von Buchstaben und Zahlen, die im BitLocker-Wiederherstellungsfenster auf dem Endpunkt einsehbar ist.

Unter Windows ist die Wiederherstellungsschlüssel-ID eine Folge von Buchstaben und Zahlen, die im BitLocker-Wiederherstellungsfenster auf dem Endpunkt einsehbar ist.

Alternativ können Sie die Option **Wiederherstellung** im Reiter **Schutz** der **Computerdetails** wählen, um die Wiederherstellungsschlüssel-ID automatisch einzufügen. Das funktioniert sowohl unter Windows als auch unter macOS.

- b. Das Passwort Ihres GravityZone-Kontos.

4. Klicken Sie auf **Anzeigen**. Das Fenster wird vergrößert.

Unter **Laufwerksinformationen** werden die folgenden Daten aufgeführt:

- a. Name des Laufwerks
- b. Laufwerktyp (bootfähig oder nicht bootfähig).
- c. Endpunkt-Name (wie im Netzwerkinventar aufgeführt)
- d. Wiederherstellungsschlüssel. Unter Windows ist der Wiederherstellungsschlüssel ein Passwort, das bei der Verschlüsselung des Laufwerks automatisch generiert wird. Unter macOS ist der Wiederherstellungsschlüssel das Passwort des Benutzerkontos.

5. Schicken Sie dem Endpunkt-Benutzer den Wiederherstellungsschlüssel.

Details zur Verschlüsselung und Entschlüsselung von Laufwerken mit GravityZone finden Sie hier: „[Verschlüsseln](#)“ (S. 401).

6.2.9. Synchronisation mit Active Directory

Das Netzwerkinventar wird automatisch nach einem im Konfigurationsbereich des Control Center festgelegten Intervall mit Active Directory synchronisiert. Weitere

Informationen finden Sie im Kapitel "GravityZone Installation und Einrichtung" der GravityZone-Installationsanleitung.

So synchronisieren Sie manuell das aktuell angezeigte Netzwerkinventar mit Active Directory:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Computer and virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Klicken Sie auf die Schaltfläche **Mit Active Directory synchronisieren** am oberen Rand der Tabelle.
4. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.



Beachten Sie

Bei großen Active-Directory-Netzwerken kann die Synchronisation eine Weile dauern.

6.3. Virtuelle Maschinen

Sie können die virtuelle Infrastruktur unter Ihrem Konto anzeigen, indem Sie zur Seite **Netzwerk** gehen und **Virtuelle Maschinen** aus der **Ansichtsauswahl** wählen.



Beachten Sie

Verwalten können Sie virtuelle Maschinen auch in der Ansicht **Computer und Virtuelle Maschinen**, die virtuelle Infrastruktur anzeigen und ihren Inhalt nach bestimmten Kriterien filtern können sie aber nur in der Ansicht **Virtuelle Maschinen**.

Weitere Informationen zum Umgang mit den Netzwerkanalysen finden Sie unter „Mit Netzwerkanalysen arbeiten“ (S. 46).

Name	Betriebssystem	IP	Zuletzt gesehen	Bezeichnung
<input type="checkbox"/> VMware-Inventar			N/A	N/A
<input type="checkbox"/> Benutzerdefinierte Gruppen			N/A	N/A
<input type="checkbox"/> Gelöscht			N/A	N/A

Das Netzwerk - Virtuelle-Maschinen-Ansicht

Im linken Fenster sehen Sie das verfügbare Netzwerk virtueller Maschinen und im rechten Fenster Details zu jeder virtuellen Maschine.

So passen Sie die Details der virtuellen Maschinen an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **III Spalten** rechts oben im rechten Fenster.
2. Wählen Sie die Spalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um zur Standardansicht zurückzukehren.

Das linke Fenster zeigt eine baumartige Ansicht der virtuellen Infrastruktur. Die Wurzel des Baums heißt **Virtuelle Maschinen**, und die virtuellen Maschinen sind nach den folgenden Kategorien (je nach eingesetzter Virtualisierungstechnologie) unter der Wurzel angeordnet:

- **Nutanix-Inventar.** Enthält die Liste der Nutanix Prism Element-Systeme, auf die Sie Zugriff haben.
- **VMware-Inventar.** Beinhaltet die Liste der vCenter-Server, auf die Sie Zugriff haben.
- **Citrix-Inventar.** Beinhaltet die Liste der XenServer-Systeme, auf die Sie Zugriff haben.
- **Benutzerdefinierte Gruppen.** Enthält die in Ihrem Netzwerk gefundenen Security Server und virtuellen Maschinen außerhalb eines vCenter-Server- oder XenServer-Systems.

Im linken Fenster gibt es auch ein Menü namens **Ansichten**, in dem der Benutzer für jeden Virtualisierungstechnologieanbieter einen Ansichtstyp auswählen kann.

Um auf die mit dem Control Center integrierte virtualisierte Infrastruktur zugreifen zu können, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare vCenter-Server-System angeben. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen. Weitere Informationen finden Sie unter [„Zugangsdaten-Manager“ \(S. 223\)](#).

Im Bereich **Netzwerk** stehen Ihnen folgende Verwaltungsoptionen für virtuelle Maschinen zur Verfügung:

- [Status virtueller Maschinen überprüfen](#)
- [Details virtueller Maschinen anzeigen](#)

- Virtuelle Maschinen in Gruppen organisieren
- Sortieren, filtern und suchen
- Aufgaben ausführen
- Schnellberichte erstellen
- Regeln zuweisen
- Lizenzplätze freigeben

Im Abschnitt **Konfiguration > Netzwerkeinstellungen** können Sie [geplante Regeln für das automatische Löschen ungenutzter virtueller Maschinen](#) aus dem Netzwerkinventar konfigurieren.

6.3.1. Status virtueller Maschinen überprüfen

Jede virtuelle Maschine wird auf der Netzwerkseite ihrem Typ und Status entsprechend durch ein Symbol dargestellt.





Unter „[Netzwerkobjekttypen und -status](#)“ (S. 543) finden Sie eine Liste aller Symbole und Status.

Detaillierte Statusinformationen finden Sie unter:

- [Verwaltungsstatus](#)
- [Verbindungsstatus](#)
- [Sicherheitsstatus](#)



Verwaltungsstatus

Virtuelle Maschinen können einen der folgenden Verwaltungsstatus haben:

-  **Verwaltet** - Virtuelle Maschinen, auf denen Bitdefender-Schutz installiert ist.
-  **Neustart steht aus** - virtuelle Maschinen, die nach Installation oder Aktualisierung von Bitdefender-Schutz einen Systemneustart erfordern.
-  **Unverwaltet** - Erkannte virtuelle Maschinen, auf denen Bitdefender-Schutz nicht installiert ist.
-  **Gelöscht** - virtuelle Maschinen, die Sie aus dem Control Center gelöscht haben. Weitere Informationen finden Sie unter „[Endpunkte aus dem Netzwerkinventar löschen](#)“ (S. 218).

Verbindungsstatus

Der Verbindungsstatus betrifft verwaltete virtuelle Maschinen und Security Server. In dieser Hinsicht können verwaltete virtuelle Maschinen entweder online oder offline sein:

-  **Online.** Ein blaues Symbol zeigt an, dass die Maschine online ist.
-  **Offline.** Ein graues Symbol zeigt an, dass die Maschine offline ist.

Eine virtuelle Maschine gilt als offline, wenn der Sicherheitsagent länger als 5 Minuten inaktiv ist. Mögliche Gründe, warum virtuelle Maschinen als offline angezeigt werden:

- Die virtuelle Maschine ist ausgeschaltet, im Ruhezustand oder im Energiesparmodus.



Beachten Sie

Virtuelle Maschinen werden auch dann als online angezeigt, wenn sie gesperrt sind oder der Benutzer sich abgemeldet hat.

- Der Sicherheitsagent hat keine Verbindung zum GravityZone-Kommunikationsserver:
 - Die Verbindung der virtuellen Maschine zum Netzwerk könnte unterbrochen worden sein.
 - Eine Netzwerk-Firewall oder ein Router könnte die Kommunikation zwischen dem Sicherheitsagenten und dem Bitdefender Control Center oder dem zugewiesenen Endpoint Security Relay blockieren.
 - Die virtuelle Maschine befindet sich hinter einem Proxy-Server, und in der zugewiesenen Richtlinie wurden die Proxy-Einstellungen nicht korrekt konfiguriert.



Warnung

Bei virtuellen Maschinen hinter einem Proxy-Server müssen die Proxy-Einstellungen im Installationspaket des Sicherheitsagenten korrekt konfiguriert sein, da die virtuelle Maschine sonst nicht mit der GravityZone kommunizieren kann und immer als offline angezeigt wird, selbst wenn nach der Installation [eine Richtlinie mit den korrekten Proxy-Einstellungen](#) angewendet wird.

- Der Sicherheitsagent wurde manuell von der virtuellen Maschine deinstalliert, während diese nicht mit dem Bitdefender Control Center oder dem zugewiesenen

Endpoint Security Relay verbunden war. Normalerweise wird das Control Center über die manuelle Deinstallation des Sicherheitsagenten von einer virtuellen Maschine benachrichtigt und die virtuelle Maschine wird als nicht verwaltet gekennzeichnet.

- Der Sicherheitsagent funktioniert unter Umständen nicht richtig.

So finden Sie heraus, wie lange virtuelle Maschinen inaktiv waren:

1. Zeigen Sie nur verwaltete virtuelle Maschinen an: Klicken Sie am oberen Rand der Tabelle auf das Menü **Filter**, wählen Sie im Reiter **Sicherheit** alle gewünschten "Verwaltet"-Optionen, markieren Sie dann im Reiter **Tiefe** die Option **Alle Objekte rekursiv** und klicken Sie anschließend auf **Speichern**.
2. Klicken Sie auf die Spaltenüberschrift **Zuletzt gesehen**, um die virtuellen Maschinen nach dem Zeitraum ihrer Inaktivität zu sortieren.

Sie können kürzere Inaktivitätszeiträume (Minuten, Stunden) ignorieren, da diese vermutlich auf ein temporäres Problem zurückzuführen sind. Die virtuelle Maschine ist zum Beispiel gerade ausgeschaltet.

Längere Inaktivitätszeiträume (Tage, Wochen) deuten in der Regel auf ein Problem mit der virtuellen Maschine hin.



Beachten Sie

Wir empfehlen, die Netzwerktabelle immer mal wieder **neu zu laden**, damit die jeweils aktuellen Daten angezeigt werden.

Sicherheitsstatus

Der Sicherheitsstatus betrifft verwaltete virtuelle Maschinen und Security Server. Virtuelle Maschinen oder Security Server mit Sicherheitsproblemen erkennen Sie daran, dass ein Warnsymbol am Statussymbol angezeigt wird:

- Mit Problemen.
- Keine Probleme.

Eine virtuelle Maschine oder ein Security Server hat dann Sicherheitsprobleme, wenn mindestens einer der folgenden Punkte zutrifft:

- Der Malware-Schutz ist deaktiviert (nur bei virtuellen Maschinen).
- Der Lizenzzeitraum ist abgelaufen.
- Das Bitdefender-Produkt ist veraltet.
- Die Sicherheitsinhalte sind veraltet.

- Das HVI-Ergänzungspaket ist veraltet.
- Malware wurde erkannt (nur bei virtuellen Maschinen).
- Die Verbindung mit Bitdefender Cloud Services konnte nicht hergestellt werden. Mögliche Gründe hierfür sind:
 - Die virtuelle Maschine hat Probleme mit der Internetverbindung.
 - Eine Netzwerk-Firewall blockiert die Verbindung mit Bitdefender Cloud Services.
 - Port 443, der für die Kommunikation mit Bitdefender Cloud Services verwendet wird, ist geschlossen.

In diesem Fall läuft der Malware-Schutz allein auf Grundlage der lokalen Engines. Cloud-Scans sind ausgeschaltet. Das heißt, dass der Sicherheitsagent keinen umfassenden Echtzeitschutz gewährleisten kann.

Wenn Ihnen eine virtuelle Maschine mit Sicherheitsproblemen auffällt, klicken Sie auf ihren Namen, um das Fenster **Informationen** anzuzeigen. Sicherheitsprobleme erkennen Sie an diesem **!** Symbol. Vergessen Sie dabei nicht, in jedem einzelnen **Reiter der Informationseite** nach Sicherheitsinformationen zu suchen. Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen. Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.

i Beachten Sie

Wir empfehlen, die Netzwerktabelle immer mal wieder **neu zu laden**, damit die jeweils aktuellen Daten angezeigt werden.

Endpunkte, die in den letzten 24 Stunden keine Updates erhalten haben, werden automatisch als **Mit Problemen** markiert. Dies geschieht unabhängig von der vorhandenen Sicherheitsinhalten auf dem Relais oder dem GravityZone Update Server.

6.3.2. Details virtueller Maschinen anzeigen

Gehen Sie folgendermaßen vor, um Details zu den einzelnen virtuellen Maschinen auf der **Netzwerkseite** abzurufen:

- **Aufrufen der Netzwerkseite**
- **Aufrufen des Informationsfensters**

Aufrufen der Netzwerkseite

Detailinformationen zu einer virtuellen Maschine finden Sie auf der **Netzwerkseite** in der Tabelle im Fenster rechts.

Mit einem Klick auf die Schaltfläche **III Spalten** oben rechts im Fenster können Sie Spalten mit Informationen zu der virtuellen Maschine hinzufügen oder entfernen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
Alle in der ausgewählten Gruppe verfügbaren virtuellen Maschinen werden in der Tabelle im rechten Fenster angezeigt.
4. Der Status einer virtuellen Maschine ist durch ein Symbol klar gekennzeichnet. Detaillierte Informationen finden Sie unter „**Status virtueller Maschinen überprüfen**“ (S. 111).
5. Die einzelnen Spalten der Tabelle enthalten verschiedene Informationen zu jeder virtuellen Maschine.

Über die Kopfzeile können Sie je nach verfügbaren Kriterien eine inkrementelle Suche nach bestimmten virtuellen Maschinen starten:

- **Name:** Name der virtuellen Maschine.
- **FQDN:** der sog. Fully Qualified Domain Name (vollständig qualifizierte Domainname), der den Host-Namen und den Domain-Namen beinhaltet.
- **Betriebssystem:** auf der virtuellen Maschine installiertes Betriebssystem.
- **IP:** IP-Adresse der virtuellen Maschine.
- **Zuletzt gesehen:** Datum und Zeitpunkt, zu denen die virtuelle Maschine zuletzt online gesehen wurde.



Beachten Sie

Sie sollten regelmäßig das Feld **Zuletzt gesehen** überprüfen, da lange Zeiträume der Inaktivität bedeuten können, dass Kommunikationsprobleme vorliegen oder die virtuelle Maschine vom Netzwerk getrennt wurde.

- **Bezeichnung:** Benutzerdefinierte Zeichenfolge mit zusätzlichen Informationen zum Endpunkt. Sie können im **Informationsfenster** einer virtuellen Maschine eine Bezeichnung hinzufügen und Sie später in Ihren Suchen verwenden.
- **Richtlinie:** Die auf die virtuelle Maschine angewandte Richtlinie, mit einem Link zum Anzeigen und Anpassen der Richtlinieneinstellungen.

Aufrufen des Informationsfensters

Klicken auf der **Netzwerkseite** im Fenster rechts auf den Namen der virtuellen Maschine, die Sie im **Informationsfenster** anzeigen möchten. In diesem Fenster werden nur die für die ausgewählte virtuelle Maschine verfügbaren Daten nach unterschiedlichen Reitern sortiert angezeigt.

Im Folgenden finden Sie die vollständige Auflistung aller Informationen, die im **Informationsfenster** zu finden sind, nach Maschinentyp (virtuelle Maschine, Security Server-Instanz) und den dazugehörigen Sicherheitsinformationen.

Reiter „Allgemein“

- Allgemeine Informationen zur virtuellen Maschine wie Name, FQDN-Informationen, IP-Adresse, Betriebssystem, Infrastruktur, übergeordnete Gruppe und aktueller Verbindungsstatus.

In diesem Bereich können Sie der virtuellen Maschine eine Bezeichnung zuweisen. So können Sie virtuelle Maschinen mit der gleichen Bezeichnung schnell und bequem finden und dort Aktionen ausführen, unabhängig davon, wo im Netzwerk sie sich befinden. Weitere Informationen zu den Filtern für virtuelle Maschinen finden Sie im Kapitel [„Sortieren, Filtern und Suchen von virtuellen Maschinen“](#) (S. 125).

- **HVI-Voraussetzungen**, liefert Informationen darüber, ob der Security Server für HVI-Schutz genutzt werden kann. Wenn der Host des Security Server auf einer unterstützten XenServer-Version läuft und das Ergänzungspaket installiert ist, können Sie HVI über diesen Host auf virtuellen Maschinen aktivieren.
- Informationen zu den Schutzebenen, einschließlich einer Liste der Sicherheitstechnologien, die Sie mit Ihrer GravityZone-Lösung erworben haben, und ihren Lizenzstatus. Folgende Status sind möglich:
 - **Verfügbar / Aktiv** – Der Lizenzschlüssel für diese Schutzebene ist auf der virtuellen Maschine aktiv.
 - **Abgelaufen** – Der Lizenzschlüssel für diese Schutzebene ist abgelaufen.
 - **Ausstehend** – der Lizenzschlüssel wurde noch nicht bestätigt.



Beachten Sie

Weitere Informationen zu den Schutzebenen finden Sie im Reiter **Schutz**.

- **Relaisverbindung:** Der Name, die IP und die Bezeichnung des Relais, mit dem die virtuelle Maschine ggf. verbunden ist.

Informationen ✕

Allgemein Schutz Richtlinie Scan-Protokolle

Virtuelle Maschine		Schutzebenen	
Name:	192_168_2_251	Endpunkt:	Aktiv
FQDN:	192_168_2_251		
IP:	10.17.47.155		
Betriebssystem:	Windows Server 2008 R2 Enterprise		
Bezeichnung:	<input type="text"/>		
Infrastruktur:	Benutzerdefinierte Gruppen		
Gruppe:	Custom Groups		
Zustand:	Offline		
Zuletzt gesehen:	23 Oktober 2017, 06:53:17		

Speichern Schließen

Fenster Informationen - Reiter Allgemein


Reiter Schutz


In diesem Reiter finden Sie Details zu jeder auf dem Endpunkt lizenzierten Schutzebene. Angezeigt werden Details zu:

- Informationen zum Sicherheitsagenten, so zum Beispiel Produktname und -version, Konfiguration der Scan-Engines sowie Update-Status. Für den Exchange-Schutz sind zudem auch Informationen zu Spam-Schutz-Engine und Signaturversionen verfügbar.
- Sicherheitsstatus für jede Schutzebene. Dieser Status wird rechts neben dem Namen der Schutzebene angezeigt:
 - **Sicher**, d. h. auf den Endpunkten, auf denen die Schutzebene angewandt wird, liegen keine Sicherheitsprobleme vor.
 - **Angreifbar**, d. h. auf den Endpunkten, auf denen die Schutzebene angewandt wird, liegen Sicherheitsprobleme vor. Weitere Informationen finden Sie unter „Sicherheitsstatus“ (S. 113).
- Zugehörige Security Server. Jeder zugewiesene Security Server wird bei agentenlosen Installationen angezeigt oder dann, wenn die Scan-Engines der

Sicherheitsagenten für die Verwendung vom Remote-Scan konfiguriert wurden. Security Server-Informationen helfen bei der Identifikation der virtuellen Appliance und dem Einholen des Update-Status.

- Informationen im Zusammenhang mit NSX, so zum Beispiel Virus-Tag-Status und die Sicherheitsgruppe, der die virtuelle Maschine zugeordnet ist. Wurde ein Sicherheits-Tag angewendet, informiert es Sie darüber, dass der Computer infiziert ist. Andernfalls ist der Computer sauber oder es werden keine Sicherheits-Tags verwendet.
- Status der Sicherheitsmodule. Hier sehen Sie, welche Sicherheitsmodule auf dem Endpunkt installiert wurden, und welchen Status die verfügbaren Module (**Ein/Aus**) gemäß der angewendeten Richtlinie haben.
- Ein schneller Überblick über die Modulaktivität und Malware-Berichte des aktuellen Tages.

Klicken Sie auf den  **Anzeigen**-Link, um die Berichtsoptionen anzuzeigen und den Bericht anzulegen. Weitere Informationen finden Sie unter „[Berichte erstellen](#)“ (S. 459)

- Informationen zum Sandbox Analyzer:
 - Sandbox Analyzer-Verwendungsstatus auf der virtuellen Maschine, wird rechts im Fenster angezeigt:
 - **Aktiv:** Der Sandbox Analyzer ist lizenziert (verfügbar) und wurde per Richtlinie auf der virtuellen Maschine aktiviert.
 - **Inaktiv:** Der Sandbox Analyzer ist lizenziert (verfügbar), wurde aber nicht per Richtlinie auf der virtuellen Maschine aktiviert.
 - Name des Agenten, der als Einspeisungssensor fungiert.
 - Modulstatus auf der virtuellen Maschine:
 - **An** - Der Sandbox Analyzer wurde per Richtlinie auf der virtuellen Maschine aktiviert.
 - **Aus** - Der Sandbox Analyzer wurde nicht per Richtlinie auf der virtuellen Maschine aktiviert.
 - Bedrohungsfunde in der letzten Woche (über einen Klick auf  **Ansicht** zur Anzeige des Berichts).
- Weitergehende Informationen zum Verschlüsselungsmodul, darunter:

- Gefundene Laufwerke (mit Kennzeichnung des Boot-Laufwerks)
- Verschlüsselungsstatus für jedes Laufwerk (also **Verschlüsselt**, **Verschlüsselung wird durchgeführt**, **Entschlüsselung wird durchgeführt**, **Nicht verschlüsselt**, **Verriegelt** oder **Angehalten**).

Klicken Sie auf den Link **Wiederherstellung**, um den Wiederherstellungsschlüssel für das entsprechende verschlüsselte Laufwerk abzurufen. Weitere Details zum Abrufen von Wiederherstellungsschlüsseln finden Sie hier: [„Der Wiederherstellungsmanager für verschlüsselte Laufwerke“](#) (S. 171).

Informationen ✕

Allgemein **Schutz** Richtlinie Scan-Protokolle

Endpunktschutz Angreifbar !

B Agent

Typ: BEST

Produktversion: 6.2.25.944

Letzte: 21 Oktober 2017 15:37:35

Produktaktualisierung:

Signaturenversion: **7.73532 !**

Letztes Signatur-Update: 21 Oktober 2017 13:35:58

Primäre Scan-Engine: Lokaler Scan

Ausweich-Scan-Engine: Keine

+ Produktübersicht

<p>❖ Module</p> <p>Malware-Schutz: An</p> <p>Gerätesteuerung: Aus</p> <p>Advanced Threat Control: An</p>	<p>📄 Berichte (heute)</p> <p>Malware-Status: Anschritt 🕒</p> <p style="padding-left: 20px;">-> Keine Funde</p> <p>Malware-Aktivität: Anschritt 🕒</p> <p style="padding-left: 20px;">-> Keine Aktivität</p>
---	--

Speichern Schließen

Fenster Informationen - Reiter Schutz

Für Security Server finden Sie in diesem Reiter Informationen zum Speicherschutzmodul. Angezeigt werden Details zu:

- Dienststatus:
 - **N/V** – Für den Speicherschutz liegt eine Lizenz vor, der Dienst wurde aber noch nicht konfiguriert.
 - **Aktiviert** – der Dienst wurde in der Richtlinie aktiviert und wird ausgeführt.
 - **Deaktiviert** – der Dienst wird nicht ausgeführt, weil er in der Richtlinie deaktiviert wurde oder der Lizenzschlüssel abgelaufen ist.

- Liste der verbundenen ICAP-konformen Speichergeräte mit den folgenden Details:
 - Name des Speichergeräts
 - IP-Adresse des Speichergeräts
 - Art des Speichergeräts
 - The date and time of the last communication between the storage device and Security Server.

Reiter Richtlinie

Auf einer virtuellen Maschine können mehrere Richtlinien angewandt werden, es kann jedoch immer nur eine der Richtlinien aktiv sein. Im Reiter **Richtlinie** werden Informationen zu allen Richtlinien angezeigt, die auf der virtuellen Maschine angewandt wurden.

- Name der aktiven Richtlinie. Klicken Sie auf den Namen der Richtlinie, um die Richtlinienvorlage und ihre Einstellungen anzuzeigen.
- Der aktive Richtlinientyp, möglich sind:
 - **Gerät**, d. h. die Richtlinie wurde der virtuellen Maschine von Netzwerkadministrator manuell zugewiesen.
 - **Standort**, d. h. eine regelbasierte Richtlinie, die der virtuellen Maschine automatisch zugewiesen wird, wenn die Netzwerkeinstellungen der virtuellen Maschine mit den Bedingungen einer bestehenden [Zuweisungsregel](#) übereinstimmen.
 - **Benutzer**, d. h. eine regelbasierte Richtlinie, die dem Endpunkt automatisch zugewiesen wird, wenn dieser mit dem Active-Directory-Ziel übereinstimmt, das mit einer bestehenden Zuweisungsregel festgelegt wurde.
Eine Maschine kann beispielsweise über zwei zugewiesene benutzerbezogene Richtlinien verfügen, eine für Administratoren und eine für andere Mitarbeiter. Eine Richtlinie wird gültig, wenn der Benutzer mit den entsprechenden Rechten sich anmeldet.
 - **Extern (NSX)**, d. h. die Richtlinie ist in der VMware-NSX-Umgebung definiert.
- Der aktive Richtlinienzuweisungstyp, möglich sind:
 - **Direkt**, d. h. die Richtlinie wird direkt auf der virtuellen Maschine angewandt.
 - **Geerbt**, d. h. die virtuelle Maschine erbt die Richtlinie von einer übergeordneten Gruppe.

- Anzuwendende Richtlinien:** Zeigt die Liste der Richtlinien an, die mit bestehenden Zuweisungsregeln verknüpft sind. Diese Richtlinien werden unter Umständen auf der virtuellen Maschine angewandt, wenn diese mit den Bedingungen der verknüpften Zuweisungsregeln übereinstimmt.

Informationen
✕

Allgemein Schutz Richtlinie Scan-Protokolle

Details

Aktive Richtlinie: rv

Typ: Gerät

Zuweisung: Direkt

Zugewiesene Regeln

Name der Richtlinie	Status	Typ	Zuweisungsregeln
rv	Angewendet	Gerät	N/A

Erste Seite — Seite von 1 — Letzte Seite 1 Objekt(e)

Speichern
Schließen

Fenster Informationen - Reiter Richtlinie

Weitere Informationen zu den Richtlinien finden Sie unter „[Policies verwalten](#)“ (S. 228)

Reiter Relais

Der Reiter **Relais** steht nur für virtuelle Maschinen mit Relais-Rolle zur Verfügung. In diesem Reiter werden Informationen über Endpunkte angezeigt, die mit dem Relais verbunden sind, z. B. Name, IP-Adresse und Bezeichnung.



Informationen
✕

Allgemein Schutz Richtlinie Relais Scan-Protokolle

Verbundene Endpunkte

Endpunkt-Name	IP	Bezeichnung
CONN-BD	192.168.12.101	
CONN-WIN	192.168.12.222	

Erste Seite
← Seite 0 von 0
→ Letzte Seite
20
0 Objekte

Speichern
Schließen

Fenster Informationen - Reiter Relais

Reiter Scan-Protokolle

Im Reiter **Scan-Protokolle** werden detaillierte Informationen zu allen Scan-Aufgaben angezeigt, die auf der virtuellen Maschine ausgeführt wurden.

Protokolle werden nach Schutzebene geordnet. Über das Klappenmenü können Sie entscheiden, für welche Ebene Protokolle angezeigt werden sollen.

Klicken Sie auf die gewünschte Scan-Aufgabe, um das Protokoll in einem neuen Reiter im Browser zu öffnen.

Wenn mehrere Scan-Protokolle zur Verfügung stehen, können Sie sich über mehrere Seiten erstrecken. Über die Navigation am unteren Rand der Tabelle können Sie zwischen den Seiten wechseln. Wenn Sie sehr viele Einträge haben, können Sie die Filteroptionen über der Tabelle nutzen.

Informationen

Allgemein Schutz Richtlinie **Scan-Protokolle**

Verfügbare Scan-Protokolle

Prüfberichte anzeigen für: Endpoint Protection

Typ	Erstellt
Speicher-Scan 2017-10-25	25 Oktober 2017, 14:09:01

Erste Seite ← Seite 1 von 1 → Letzte Seite 20 2 Objekt(e)

Speichern Schließen

Fenster Informationen - Reiter Scan-Protokolle

Jede Eigenschaft in diesem Fenster, von der Sicherheitsprobleme ausgehen, ist mit dem **!**-Symbol gekennzeichnet. Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen. Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.

6.3.3. Virtuelle Maschinen in Gruppen organisieren

Im linken Fenster der Seite **Netzwerk** können Sie im Ordner **Benutzerdefinierte Gruppen** die Gruppen virtueller Maschinen verwalten.

Virtuelle Maschinen, die aus Nutanix Prism Element importiert worden sind, finden sich im Ordner **Nutanix-Inventar**. Virtuelle Maschinen, die von VMware vCenter importiert worden sind, finden sich im Ordner **VMware-Inventar**. Virtuelle Maschinen, die von XenServer importiert worden sind, finden sich im Ordner **Citrix-Inventar**. Sie können das Nutanix-Inventar, das VMware-Inventar oder das Citrix-Inventar nicht bearbeiten. Sie können nur die zugehörigen virtuellen Maschinen anzeigen und verwalten.

Alle virtuellen Maschinen, die weder von Nutanix Prism-, vCenter- oder XenServer-Systemen verwaltet werden, werden von der Netzwerkerkennung gefunden und in den Ordner **Benutzerdefinierte Gruppen** sortiert, in dem Sie sie nach Belieben in Gruppen organisieren können. Ein großer Vorteil ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Unter **Benutzerdefinierte Gruppen** können Sie Gruppen virtueller Maschinen innerhalb einer benutzerdefinierten Baumstruktur **erstellen**, **löschen**, **umbenennen** und **verschieben**.



Beachten Sie

- Eine Gruppe kann sowohl virtuelle Maschinen als auch andere Gruppen enthalten.
- Wenn Sie im linken Bereich eine Gruppe auswählen, können Sie alle enthaltenen virtuellen Maschinen einsehen - ausgenommen der, die in die jeweiligen Untergruppen eingeordnet wurden. Wenn Sie alle virtuellen Maschinen der Gruppe und ihrer Untergruppen anzeigen möchten, klicken Sie auf das Menü **Filter** am oberen Rand der Tabelle und wählen Sie **Alle Objekte rekursiv** im Bereich **Tiefe**.

Gruppen erstellen

Bevor Sie Gruppen erstellen, sollten Sie sich überlegen, warum Sie diese Gruppen brauchen und sie dann nach einem bestimmten System erstellen. Sie können virtuelle Maschinen zum Beispiel anhand von einem oder einer Kombination der folgenden Kriterien in Gruppen einteilen:

- Organisationsstruktur (Vertrieb, Marketing, Qualitätssicherung, Software-Entwicklung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Um Ihr Netzwerk in Gruppen aufzuteilen:

1. Wählen Sie **Benutzerdefinierte Gruppen** im linken Fenster.
2. Klicken Sie auf die Schaltfläche **+ Gruppe hinzufügen** im oberen Bereich des linken Fensters.
3. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK**. Die neue Gruppe wird jetzt unter **Benutzerdefinierte Gruppen** angezeigt.

Gruppen umbenennen

So benennen Sie eine Gruppe um:

1. Wählen Sie im linken Fenster die Gruppe aus.
2. Klicken Sie auf die Schaltfläche **🔗 Gruppe bearbeiten** im oberen Bereich des linken Fensters.

3. Geben Sie den neuen Namen in das entsprechende Feld ein.
4. Klicken Sie zur Bestätigung auf **OK**.

Gruppen und virtuelle Maschinen verschieben

Innerhalb der Hierarchie **Benutzerdefinierte Gruppen** können Sie Entitäten beliebig verschieben. Ziehen Sie die gewünschte Entität einfach mit der Maus aus dem rechten Fenster in die gewünschte Gruppe im linken Fenster.



Beachten Sie

Die verschobene Entität erbt dabei die Richtlinieneinstellungen der neuen übergeordneten Gruppe, es sei denn, die Richtlinienerbung wurde deaktiviert und eine andere Richtlinie zugewiesen. Weitere Informationen über Richtlinienerbung finden Sie unter „[Sicherheitsrichtlinien](#)“ (S. 227).

Gruppen löschen

Eine Gruppe kann nicht gelöscht werden, wenn Sie mindestens eine virtuelle Maschine enthält. Wenn Sie eine Gruppe löschen möchten, verschieben Sie zunächst alle virtuellen Maschinen in (eine) andere Gruppe(n). Wenn die Gruppe Untergruppen enthält, können Sie anstelle von einzelnen virtuellen Maschinen auch ganze Untergruppen verschieben.

Um eine Gruppe zu löschen:

1. Wählen Sie die leere Gruppe.
2. Klicken Sie auf die Schaltfläche  **Gruppe entfernen** im oberen Bereich des linken Fensters. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

6.3.4. Sortieren, Filtern und Suchen von virtuellen Maschinen

Je nach Anzahl der virtuellen Maschinen kann sich die Tabelle über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt). Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Bei zu vielen Einträgen können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das **Filter**-Menü im oberen Bereich der Tabelle verwenden, um nur die Einträge

anzuzeigen, die Sie interessieren. So können Sie zum Beispiel nach einer bestimmten virtuellen Maschine suchen oder nur verwaltete virtuelle Maschinen anzeigen.

Virtuelle Maschinen sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Wenn Sie zum Beispiel möchten, dass die virtuellen Maschinen nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**. Wenn Sie erneut auf den Titel klicken, werden die virtuellen Maschinen in umgekehrter Reihenfolge angezeigt.

Name	Betriebssystem	IP	Zuletzt gesehen	Bezeichnung

Computer sortieren

Virtuelle Maschinen filtern

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Klicken Sie auf das **Filter**-Menü im oberen Bereich der Netzwerkfenster.
3. So verwenden Sie die Filterkriterien:
 - **Typ.** Wählen Sie die Art der virtuellen Entitäten, die angezeigt werden sollen.

Typ
Sicherheit
Richtlinie
Betrieb
Tag
Tiefe

Filtern nach

Virtuelle Maschinen

Hosts

vApps

Ordner

Cluster

Rechenzentren

Ressourcenpools

Pools

Tiefe: in den ausgewählten Ordnern

Speichern
Abbrechen
Zurücksetzen

Virtuelle Maschinen - nach Art filtern

- Sicherheit.** Wählen Sie Schutzverwaltung und/oder Sicherheitsstatus aus, um die Netzwerkobjekte danach zu filtern. So können Sie zum Beispiel nur die Security Server-Computer oder nur Endpunkte mit Sicherheitsproblemen anzeigen .

Typ	Sicherheit	Richtlinie	Tiefe	Betrieb	Tag
Verwaltung		Sicherheitsprobleme			
<input type="checkbox"/>	Verwaltet (Endpunkte)	<input type="checkbox"/>	Mit Sicherheitsproblemen		
<input type="checkbox"/>	Verwaltet (Exchange-Server)	<input type="checkbox"/>	Ohne Sicherheitsprobleme		
<input type="checkbox"/>	Verwaltet (Relais)				
<input type="checkbox"/>	Security Server				
<input type="checkbox"/>	Nicht verwaltet				
Tiefe: in den ausgewählten Ordnern					
Speichern		Abbrechen		Zurücksetzen	

Virtuelle Maschinen - nach Sicherheit filtern

- Richtlinie.** Wählen Sie die Richtlinienvorlage, nach der Sie die Virtuelle Maschine filtern möchten, den Richtlinienzuweisungstyp (direkt oder geerbt) sowie den Richtlinienzuweisungsstatus (aktiv, angewendet oder ausstehend).



Typ	Sicherheit	Richtlinie	Betrieb	Tag	Tiefe
<p>Vorlage: <input type="text"/></p> <p><input type="checkbox"/> Bearbeitet vom Power-User</p> <p>Typ: <input type="checkbox"/> Direkt <input type="checkbox"/> Geerbt</p> <p>Status: <input type="checkbox"/> Aktiv <input type="checkbox"/> Angewendet <input type="checkbox"/> Ausstehend</p> <p>Tiefe: in den ausgewählten Ordnern</p>					
Speichern		Abbrechen		Zurücksetzen	

Virtuelle Maschinen - nach Richtlinie filtern

- Versorgung.** Sie können virtuelle Maschinen anzeigen, die online und/oder offline und/oder gesperrt sind.

Typ	Sicherheit	Richtlinie	Betrieb	Tag	Tiefe
<p>Anzeigen</p> <p><input type="checkbox"/> Online <input type="checkbox"/> Offline <input type="checkbox"/> Gesperrt</p> <p>Tiefe: in den ausgewählten Ordnern</p>					
Speichern		Abbrechen		Zurücksetzen	

Virtuelle Maschinen - nach Versorgung filtern

- Tags.** Sie können die virtuellen Maschinen nach Tags und Attributen Filtern, die Sie in Ihrer Virtualisierungsumgebung definiert haben.

The screenshot shows a configuration window with tabs: Typ, Sicherheit, Richtlinie, Betrieb, Tag (selected), and Tiefe. Below the tabs is a table with columns: Typ, Attribut, Wert/Tag, and Aktionen. The table is currently empty. Below the table, it says 'Tiefe: in den ausgewählten Ordnern'. At the bottom are three buttons: 'Speichern', 'Abbrechen', and 'Zurücksetzen'.

Virtuelle Maschinen - nach Tags filtern

- **Tiefe.** Bei der Verwaltung eines Netzwerks virtueller Maschinen mit Baumstruktur werden virtuelle Maschinen, die sich in Untergruppen befinden, standardmäßig nicht angezeigt. Wählen Sie **Alle Objekte rekursiv**, um alle virtuellen Maschinen in der aktuellen Gruppe und ihrer Untergruppen anzuzeigen.

The screenshot shows a configuration window with tabs: Typ, Sicherheit, Richtlinie, Betrieb, Tag, and Tiefe (selected). Under the 'Filtern nach' section, there are two radio buttons: 'Objekte in den gewählten Ordnern' (selected) and 'Alle Objekte rekursiv'. Below this, it says 'Tiefe: in den ausgewählten Ordnern'. At the bottom are three buttons: 'Speichern', 'Abbrechen', and 'Zurücksetzen'.

Virtuelle Maschinen - nach Tiefe filtern



Beachten Sie

Klicken Sie auf **Zurücksetzen**, um den Filter herauszunehmen und alle virtuellen Maschinen anzuzeigen.

4. Klicken Sie auf **Speichern**, um die virtuellen Maschinen nach den gewählten Kriterien zu filtern.

Virtuelle Maschinen suchen

1. Wählen Sie den gewünschten Container im linken Fenster.
2. Geben Sie den Suchbegriff in das entsprechende Feld unter der Spaltenüberschrift (Name, Betriebssystem oder IP) vom rechten Fenster rein. Geben Sie zum Beispiel die IP-Adresse der virtuellen Maschine, die Sie suchen, in das Feld **IP** ein. Nur die passende virtuelle Maschine wird in der Tabelle angezeigt.

Leeren Sie das Suchfeld, um die vollständige Liste der virtuellen Maschinen anzuzeigen.

6.3.5. Aufgaben auf virtuellen Maschinen ausführen

Über die Seite **Netzwerk** können Sie per Fernzugriff eine Reihe administrativer Aufgaben auf virtuellen Maschinen ausführen.

Sie haben die folgenden Möglichkeiten:

- „Scan“ (S. 131)
- „Patch-Aufgaben“ (S. 142)
- „Exchange-Scan“ (S. 145)
- „Installieren“ (S. 149)
- „Client Deinstallieren“ (S. 154)
- „Update (Aktualisierung)“ (S. 155)
- „Client neu konfigurieren“ (S. 156)
- „Netzwerkerkennung“ (S. 158)
- „Anwendungserkennung“ (S. 158)
- „Computer neu starten“ (S. 159)
- „Security Server installieren“ (S. 160)
- „Security Server deinstallieren“ (S. 163)
- „Security Server aktualisieren“ (S. 163)
- „HVI-Ergänzungspaket installieren“ (S. 164)
- „HVI-Ergänzungspaket deinstallieren“ (S. 165)
- „HVI-Ergänzungspaket aktualisieren“ (S. 166)

Sie können Aufgaben individuell für einzelne virtuelle Maschinen oder für Gruppen von virtuellen Maschinen erstellen. Sie können zum Beispiel per Ferninstallation Bitdefender Endpoint Security Tools auf einer Gruppe von nicht verwalteten virtuellen Maschinen installieren. Später können Sie eine Scan-Aufgabe für eine bestimmte virtuelle Maschine aus dieser Gruppe erstellen.

Auf jeder virtuellen Maschine können Sie nur kompatible Aufgaben ausführen. Wenn Sie zum Beispiel eine nicht verwaltete virtuelle Maschine auswählen, können Sie nur den Sicherheitsagenten installieren; alle anderen Aufgaben sind nicht verfügbar.


Bei einer Gruppe wird die ausgewählte Aufgabe nur für kompatible virtuelle Maschinen erstellt. Wenn keine virtuelle Maschine der Gruppe mit der ausgewählten Aufgabe kompatibel ist, werden Sie benachrichtigt, dass die Aufgabe nicht erstellt werden konnte.

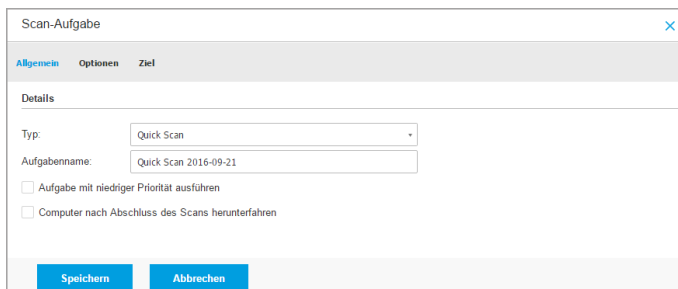
Sofort nach der Erstellung startet die Aufgabe auf virtuellen Maschinen, die online sind. Wenn eine virtuelle Maschine offline ist, wird die Aufgabe ausgeführt, sobald sie wieder online ist.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Scan

So führen Sie eine Scan-Aufgabe per Fernzugriff auf einer oder mehreren virtuellen Maschinen aus:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen für die virtuellen Maschinen, die Sie scannen möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Scan**. Ein Konfigurationsfenster wird sich öffnen.
6. Konfigurieren Sie die Scan-Optionen:
 - Im Reiter **Allgemein** können Sie den Scan-Typ auswählen und der Scan-Aufgabe einen Namen geben. Der Name dient nur dazu, den Scan auf der Seite [Aufgaben](#) leicht wiederzufinden.



Scan-Aufgabe für virtuelle Maschine - Konfigurieren der allgemeinen Einstellungen

Wählen Sie den gewünschten Typ aus dem Menü **Typ**:

- **Quick-Scan** ist so vorkonfiguriert, dass nur kritische Systemordner und neue Dateien gescannt werden. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virens캔 in Anspruch nehmen würde.

Wenn Malware oder Rootkits gefunden werden, desinfiziert Bitdefender sie automatisch. Wenn die Datei aus irgendeinem Grund nicht desinfiziert werden kann, wird sie in die Quarantäne verschoben. Dieser Art Scan ignoriert verdächtige Dateien.

- Der **Vollständige Scan** durchsucht das gesamte System nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.

Bitdefender versucht automatisch als infiziert erkannte Dateien zu desinfizieren. Sollte die Malware nicht entfernt werden können, wird sie in die Quarantäne verschoben, wo sie keinen Schaden mehr anrichten kann. Verdächtige Dateien werden ignoriert. Wenn Sie auch für verdächtige Dateien Aktionen ausführen möchten oder für infizierte Dateien andere Standardaktionen definieren möchten, führen Sie einen benutzerdefinierten Scan durch.

- **Speicher-Scan** überprüft die Programme, die im Speicher der virtuellen Maschine laufen.
- **Netzwerk-Scan** ist ein benutzerdefinierter Scan, mit dem Netzwerklaufwerke mit dem Bitdefender-Sicherheitsagenten, der auf der

ansprechenden virtuellen Maschine installiert ist, gescannt werden können.

Damit die Netzwerk-Scan-Aufgabe funktioniert, müssen folgende Voraussetzungen erfüllt sein:

- Sie müssen die Aufgabe einem einzelnen Endpunkt in Ihrem Netzwerk zuweisen.
 - Sie müssen die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann. Die nötigen Zugangsdaten können Sie im Aufgabenfenster im Reiter **Ziel** konfigurieren.
- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Für Speicher-, Netzwerk- und benutzerdefinierte Scans stehen Ihnen zudem die folgenden Optionen zur Auswahl:

- **Aufgabe mit niedriger Priorität ausführen.** Durch Anklicken dieses Kästchens setzen Sie die Priorität des Scan-Prozesses herab und ermöglichen es anderen Programmen, schneller zu laufen. Hierdurch wird die für den Scan-Prozess benötigte Zeit verlängert.



Beachten Sie

Diese Option gilt nur für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent).

- **Computer nach Abschluss des Scans herunterfahren.** Mit diesem Kästchen schalten Sie Ihren Computer aus, sofern Sie ihn eine Zeitlang nicht nutzen wollen.



Beachten Sie

Diese Option gilt für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent) und Endpoint Security for Mac.

Für benutzerdefinierte Scans müssen Sie die folgenden Einstellungen konfigurieren:

- Gehen Sie zum Reiter **Optionen**, um die Scan-Optionen festzulegen. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren. Wählen Sie dazu die Option **Benutzerdefiniert** und erweitern Sie dann den Bereich **Einstellungen**.

Scan-Aufgabe

Allgemein Optionen Ziel

Prüfoptionen

- Aggressiv Benutzerdefiniert - vom Administrator festgelegte Einstellungen

- Normal

- Tolerant

- Benutzerdefiniert

• Einstellungen

Speichern Abbrechen

Scan-Aufgabe für virtuelle Maschine - Konfiguration eines benutzerdefinierten Scans

Die folgenden Optionen stehen zur Verfügung:

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateierdung), oder nur für Anwendungsdateien oder nur für bestimmte Dateierdungen, die Sie für gefährlich erachten, durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.



Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 545).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf **Speichern**.



Wichtig

Bitdefender-Sicherheitsagenten, die auf Windows- und Linux-Systemen installiert sind, scannen die meisten ISO-Formate, führen aber keine Aktionen für sie durch.

The screenshot shows the 'Einstellungen' (Settings) window in Bitdefender GravityZone. Under the 'Dateitypen' (File Types) section, the 'Typ:' (Type) dropdown menu is set to 'Benutzerdefinierte Endungen' (Custom Extensions). Below it, the 'Erweiterungen:' (Extensions) text box contains the entries 'exe' and 'bat', with a small 'X' icon next to 'exe'.

Optionen einer Scan-Aufgabe für eine virtuelle Maschine - Hinzufügen von benutzerdefinierten Endungen

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierte Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, Archive zu scannen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.



Wichtig

Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten. Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
 - **Archivgröße begrenzen auf (MB).** Sie können die maximale Größe der Archive angeben, die gescannt werden sollen.

Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

- **Maximale Archvertiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archvertiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.
- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.



Wichtig

Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
 - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Code der virtuellen Maschine um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
 - **Registrierung scannen.** Wählen Sie diese Option, um die Registrierungsschlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
 - **Nach Rootkits suchen.** Wählen Sie diese Option, um nach **Rootkits** und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
 - **Nach Keyloggern suchen.** Wählen Sie diese Option, um nach **Keylogger**-Software zu suchen. Keylogger sind an sich keine schädlichen Anwendungen, können aber zu kriminellen Zwecken eingesetzt werden. Der Hacker kann über diese gestohlenen Daten

- sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
 - **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Browsern auf der virtuellen Maschine gespeichert werden.
 - **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
 - **Auf potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.
 - **Wechseldatenträger scannen.** Wählen Sie diese Option, um Wechseldatenträger zu scannen, die mit der virtuellen Maschine verbunden sind.
 - **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
 - **Wenn eine infizierte Datei gefunden wird.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI). Der Bitdefender-Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

Wenn eine infizierte Datei gefunden wird, versucht der Bitdefender-Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.



Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Wenn eine verdächtige Datei gefunden wird.** Dateien werden durch heuristische Analysen und andere Bitdefender-Technologien als verdächtig erkannt. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden). Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden. Dateien in Quarantäne werden zu Analyse Zwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Wenn ein Rootkit gefunden wurde.** Rootkits sind spezielle Software-Werkzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

Wird ein Virus auf einer virtuellen NSX-Maschinen gefunden, markiert Security Server die virtuelle Maschine automatisch mit einem Sicherheits-Tag. Dies setzt voraus, dass diese Option bei der vCenter-Server-Integration ausgewählt wurde.

Zu diesem Zweck enthält NSX drei Sicherheits-Tags, die dem Schweregrad der Bedrohung entsprechen:

- `ANTI_VIRUS.VirusFound.threat=niedrig` gilt für Maschinen, auf denen Bitdefender Malware mit niedrigem Risikopotenzial gefunden hat, die gelöscht werden kann.
- `ANTI_VIRUS.VirusFound.threat=mittel` gilt für Maschinen, auf denen Bitdefender die infizierten Dateien nicht löschen kann, sondern sie stattdessen desinfiziert.
- `ANTI_VIRUS.VirusFound.threat=hoch` gilt für Maschinen, auf denen Bitdefender die infizierten Dateien weder löschen noch desinfizieren kann, sondern stattdessen den Zugriff darauf blockiert.

Sie können infizierte Maschinen isolieren, indem Sie Sicherheitsgruppen mit dynamischer Mitgliedschaft auf Grundlage der Sicherheits-Tags anlegen.



Wichtig

- Wenn Bitdefender auf einem Computer Bedrohungen mit unterschiedlichen Schweregraden findet, werden alle passenden Tags angewandt.
- Ein Sicherheits-Tag wird es dann wieder von einem Computer entfernt, wenn ein vollständiger Scan durchgeführt und der Computer desinfiziert wurde.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie. Wählen Sie aus den entsprechenden Menus die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll. Folgende Aktionen stehen zur Verfügung:

Desinfizieren

Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Dateien in Quarantäne verschieben

Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die [Quarantäne](#)-Seite in der Konsole verwalten.

Löschen

Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Ignorieren

Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

- Gehen Sie zum Reiter **Ziel**, um die Speicherorte hinzuzufügen, die auf den gewünschten virtuellen Maschinen gescannt werden sollen.

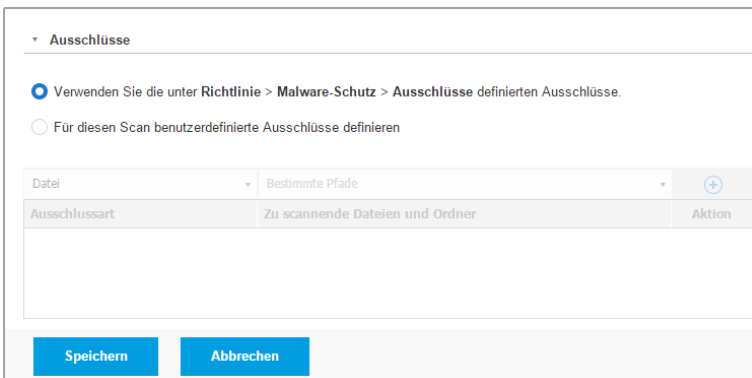
Im Bereich **Scan-Ziel** können Sie eine neue Datei oder einen neuen Ordner hinzufügen, die/der gescannt werden soll:

- a. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.
- b. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.
 - Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen. Um einen bestimmten Ordner im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.
 - Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen virtuellen Maschinen gültig ist. Weitere Informationen zu den Systemvariablen finden Sie unter „[Systemvariablen](#)“ (S. 546).
- c. Klicken Sie auf den entsprechenden [+](#) **Hinzufügen**-Link.

Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an. Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende **✕** **Löschen**-Schaltfläche.

Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.

Klicken Sie auf den Bereich **Ausschlüsse**, wenn Sie bestimmte Ziele ausschließen möchten.



Datei	Bestimmte Pfade	Aktion
Ausschlussart	Zu scannende Dateien und Ordner	Aktion

Scan-Aufgabe für virtuelle Maschinen - Festlegen von Ausschlüssen

Sie können entweder die per Richtlinie definierten Ausschlüsse verwenden oder für die aktuelle Scan-Aufgabe bestimmte Ausschlüsse definieren. Weitere Informationen finden Sie unter „[Ausschlüsse](#)“ (S. 301).

7. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).



Beachten Sie

Zum Planen von Scan-Aufgaben öffnen Sie die Seite **Richtlinien**, wählen Sie die den entsprechenden virtuellen Maschinen zugewiesene Richtlinie aus, und fügen Sie im

Bereich **Malware-Schutz** > **Bei Bedarf** eine Scan-Aufgabe hinzu. Weitere Informationen finden Sie unter „**Bedarf-Scan**“ (S. 279).

Patch-Aufgaben

Es wird empfohlen, regelmäßig zu prüfen, ob Softwareupdates zur Verfügung stehen und diese so schnell wie möglich einzuspielen. Mit GravityZone lässt sich dieser Vorgang durch Sicherheitsrichtlinien automatisieren. Wenn Sie die Software auf bestimmten virtuellen Maschinen jedoch sofort aktualisieren möchten, führen Sie die folgenden Aufgaben in dieser Reihenfolge durch:

1. [Patch-Scan](#)
2. [Patch-Installation](#)


Vorbereitende Maßnahmen

- Der Sicherheitsagent mit dem Patch-Management-Modul wurde auf den Zielmaschinen installiert.
- Damit die Scan- und Installationsaufgaben erfolgreich durchgeführt werden können, müssen auf den Windows-Maschinen die folgenden Bedingungen erfüllt sein:
 - Das **DigiCert Assured ID Root CA**-Zertifikat ist unter **Vertrauenswürdige Stammzertifizierungsstellen** gespeichert.
 - **Vorübergehende Zertifizierungsstellen** umfasst das **DigiCert SHA2 Assured ID Code Signing CA**-Zertifikat.
 - Auf den Endpunkten sind die Patches für Windows 7 und Windows Server 2008 R2 installiert, die in diesem Microsoft-Artikel erwähnt sind: [Microsoft Security Advisory 3033929](#)

Patch-Scan

Virtuelle Maschinen mit veralteter Software sind anfällig für Angriffe. Es empfiehlt sich daher, die auf Ihren Maschinen installierte Software regelmäßig zu überprüfen und Updates so schnell wie möglich einzuspielen. Gehen Sie folgendermaßen vor, um Ihre virtuellen Maschinen auf fehlende Patches zu überprüfen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).

3. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Zielendpunkte aus.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Patch-Scan** aus. Ein Bestätigungsfenster wird angezeigt.
6. Klicken Sie zur Bestätigung der Scan-Aufgabe auf **Ja**.

Nach Abschluss der Aufgabe fügt GravityZone alle von Ihrer Software benötigten Patches dem Patch-Inventar hinzu. Weitere Informationen finden Sie unter „Patch-Inventar“ (S. 205).

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „Aufgaben anzeigen und verwalten“ (S. 214).



Beachten Sie

Um einen Zeitplan für die Patch-Scans festzulegen, bearbeiten Sie die den Zielmaschinen zugewiesenen Richtlinien und konfigurieren Sie die Einstellungen im Bereich **Patch-Management**. Weitere Informationen finden Sie unter „Patch-Verwaltung“ (S. 351).

Patch-Installation

Gehen Sie folgendermaßen vor, um einen oder mehrere Patches auf den virtuellen Zielmaschinen zu installieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Patch-Installation** aus.
Ein Konfigurationsfenster wird sich öffnen. Hier können Sie alles Patches einsehen, die auf den virtuellen Zielmaschinen fehlen.
5. Nutzen Sie bei Bedarf die Sortierungs- und Filtermöglichkeiten am oberen Rand der Tabelle, um nach bestimmten Patches zu suchen.
6. Klicken Sie auf die Schaltfläche  **Spalten** oben rechts im Fenster, um nur relevante Informationen anzuzeigen.

7. Wählen Sie die Patches aus, die Sie installieren möchten.

Es gibt Patches, die von anderen Patches abhängen. Ist dies der Fall werden Sie automatisch gemeinsam mit dem entsprechenden Patch ausgewählt.

Mit einem Klick auf die Ziffern von **CVEs** oder **Produkten** wird links ein neuer Bereich angezeigt. In diesem Bereich finden Sie zusätzliche Informationen, so zum Beispiel die CVEs, die durch das Patch behoben werden und die Produkte, auf die das Patch angewendet wird. Klicken Sie auf **Schließen**, wenn Sie alles gelesen haben, um den Bereich wieder zu schließen.

8. Wählen Sie zum Neustart von Endpunkten unmittelbar nach der Patch-Installation die Option **Falls nötig, Endpunkte nach Installation des Patches neu starten**, wenn ein Systemstart erforderlich ist. Bitte bedenken Sie, dass diese Aktion Benutzer bei der Arbeit stören könnte.

9. Klicken Sie auf **Installieren**.

Die Installationsaufgabe wird gemeinsam mit allen Unteraufgaben für jede virtuelle Zielmaschine erstellt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“](#) (S. 214).

Beachten Sie

- Um einen Zeitplan für die Patch-Installation festzulegen, bearbeiten Sie die den Zielmaschinen zugewiesenen Richtlinien und konfigurieren Sie die Einstellungen im Bereich **Patch-Management**. Weitere Informationen finden Sie unter [„Patch-Verwaltung“](#) (S. 351).
- Sie können für Sie interessante Patches zudem über die Seite **Patch-Inventar** installieren. Wählen Sie dazu das Patch aus der Liste aus, klicken Sie am oberen Rand der Tabelle auf **Installieren** und konfigurieren Sie die Installationsdetails. Weitere Informationen finden Sie unter [„Installieren von Patches“](#) (S. 209).
- Nach Installation eines Patches empfiehlt es sich, eine **Patch-Scan**-Aufgabe an die Zielendpunkte zu übermitteln. Durch diese Aktion werden die in GravityZone gespeicherten Patch-Informationen für Ihre verwalteten Netzwerke aktualisiert.

Sie haben folgende Optionen zur Deinstallation von Patches:

- Per Fernzugriff durch Übermittlung einer [Aufgabe zur Patch-Deinstallation](#) über GravityZone.

- Lokal auf der Maschine. Dazu müssen Sie sich als Administrator am Endpunkt anmelden und das Deinstallationsprogramm manuell ausführen.

Exchange-Scan

Sie können die Datenbank eines Exchange-Servers aus der Ferne scannen, indem Sie eine **Exchange-Scan**-Aufgabe ausführen.

Damit der Scan einer Exchange-Datenbank durchgeführt werden kann, müssen Sie Bedarf-Scans aktivieren, indem Sie die Zugangsdaten eines Exchange-Administrators eingeben. Weitere Informationen finden Sie unter „[Scannen des Exchange-Informationsspeichers](#)“ (S. 377).

So scannen Sie eine Exchange-Server-Datenbank:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe aus, die den gewünschten Exchange-Server enthält. Sie finden den Server dann im rechten Fenster.



Beachten Sie

Sie können auch Filter verwenden, um den gewünschten Server schneller zu finden:

- Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Verwaltet (Exchange-Server)** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.
 - Geben Sie den Hostnamen oder die IP-Adresse des Servers in die Felder der entsprechenden Spaltenüberschrift ein.
4. Markieren Sie das Kästchen des Exchange-Servers, dessen Datenbank Sie scannen möchten.
 5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Exchange-Scan**. Ein Konfigurationsfenster wird sich öffnen.
 6. Konfigurieren Sie die Scan-Optionen:
 - **Allgemein**. Geben Sie einen aussagekräftigen Namen für die Aufgabe ein.
Bei großen Datenbanken kann der Scan lange dauern und die Serverleistung beeinträchtigen. Markieren Sie in solchen Fällen das Kästchen **Scan stoppen, wenn er länger dauert als** und wählen Sie einen beliebigen Zeitraum aus den entsprechenden Menüs
 - **Ziel**. Hier können Sie Container und Objekte auswählen, die gescannt werden sollen. Sie können Postfächer, öffentliche Ordner oder beides scannen lassen. Außer E-Mails können Sie auch andere Objekte wie **Kontakte**,

Aufgaben, Termine und Mail-Objekte scannen lassen. Außerdem können Sie den Scan wie folgt einschränken:

- Nur ungelesene E-Mails
- Nur Objekte mit Anhängen
- Nur neue Objekte, die in einem bestimmten Zeitraum empfangen wurden

So können Sie zum Beispiel nur E-Mails in Benutzer-Postfächern scannen lassen, die in den letzten sieben Tagen empfangen wurden.

Markieren Sie das Kästchen **Ausschlüsse**, wenn Sie Scan-Ausnahmen definieren möchten. So erstellen Sie mithilfe der Felder in der Tabellenüberschrift eine Ausnahme:

- a. Wählen Sie den Repository-Typ aus dem Menü.
- b. Geben Sie je nach Repository-Typ das auszuschließende Objekt an:

Repository-Typ	Objektformat
Postfach	E-Mail-Adresse
Öffentlicher Ordner	Ordnerpfad, von Root ausgehend
Datenbank	Die Datenbankidentität



Beachten Sie

Mit dem folgenden Exchange-Shell-Befehl können Sie die Datenbankidentität abrufen:

```
Get-MailboxDatabase | fl name,identity
```

Sie können nicht mehr als ein Objekt gleichzeitig eingeben. Wenn Sie mehrere Objekte desselben Typs haben, müssen Sie für jedes einzelne Objekt eine eigene Regel definieren.

- c. Klicken Sie am oberen Rand der Tabelle auf die Schaltfläche **Hinzufügen**, um die Ausnahme zu speichern und der Liste hinzuzufügen.

Um eine Ausnahmenregel aus der Liste zu löschen, klicken Sie auf die entsprechende **Löschen**-Schaltfläche.

- **Optionen.** Hier können Sie die Scan-Optionen für E-Mails einstellen, die zu einer Regel passen:
 - **Gescannte Dateitypen.** Mit dieser Option legen Sie fest, welche Dateitypen gescannt werden. Sie können einstellen, dass alle Dateien gescannt werden (unabhängig von der Dateiendung), nur Anwendungsdateien oder nur bestimmte Dateiendungen, die Sie für gefährlich halten. Das Scannen

aller Dateien bietet den besten Schutz, nur Anwendungsdateien zu scannen ist schneller.



Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 545).

Wenn Sie nur Dateien mit bestimmten Endungen scannen möchten, haben Sie zwei Möglichkeiten:

- **Benutzerdefinierte Endungen;** geben Sie hier nur die Endungen der Dateitypen ein, die gescannt werden sollen.
- **Alle Dateien außer bestimmten Endungen;** hierbei geben sie nur die Dateieindungen ein, die nicht gescannt werden sollen.
- **Maximalgröße für Anhang/Nachrichteninhalt (in MB).** Markieren Sie dieses Kästchen und geben Sie einen Wert in das entsprechende Feld ein, um die Maximalgröße für angehängte Dateien oder Nachrichteninhalte festzulegen, bis zu der gescannt werden soll.
- **Maximale Archivtiefe (Ebenen).** Markieren Sie dieses Kästchen und wählen Sie die maximale Archivtiefe im entsprechenden Feld. Je geringer dieser Wert, desto höher die Leistung und geringer die Sicherheit.
- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Markieren Sie dieses Kästchen, um nach potenziell bösartigen oder unerwünschten Anwendungen zu scannen, z. B. Adware, die sich ohne Zustimmung des Benutzers auf dem System installiert, das Verhalten anderer Software beeinflusst oder die Systemleistung einschränkt.
- **Aktionen.** Sie können für den Sicherheitsagenten abhängig von der Erkennungsart verschiedene automatische Aktionen für Dateien festlegen.

Über die Erkennungsart werden Dateien in drei Kategorien unterteilt:

- **Infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI).
- **Verdächtige Dateien.** Diese Dateien werden durch heuristische Analyse und andere Bitdefender-Technologien als verdächtig eingestuft. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden).

- **Unscanbare Dateien.** Diese Dateien können nicht gescannt werden. So können zum Beispiel passwortgeschützte, verschlüsselte oder überkomprimierte Dateien nicht gescannt werden.

Für jeden Erkennungstyp gibt es eine Standard- oder Hauptaktion und eine alternative Aktion für den Fall, dass die Hauptaktion fehlschlägt. Es wird nicht empfohlen, aber wenn Sie möchten, können Sie diese Aktionen über die entsprechenden Menüs ändern. Wählen Sie die Aktion, die ausgeführt werden soll:

- **Desinfizieren.** Entfernt den schädlichen Code aus infizierten Dateien und rekonstruiert die Originaldatei. Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
- **E-Mail ablehnen/löschen.** Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei löschen.** Entfernt problematische Anhänge ohne Warnung. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei ersetzen.** Entfernt problematische Dateien und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert.
- **Datei in die Quarantäne verschieben.** verschiebt erkannte Dateien in den Quarantäneordner und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. In die Quarantäne verschobene Dateien können Sie auf der Seite **Quarantäne** verwalten.



Beachten Sie

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist. Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

- **Keine Aktion durchführen.** Wenn problematische Dateien gefunden werden, wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen. Scan-Aufgaben sind standardmäßig so

konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.

- Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden**.

7. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.
8. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Installieren

Um virtuelle Maschinen mit Security for Virtualized Environments zu schützen, müssen Sie den Bitdefender-Sicherheitsagenten auf jeder von ihnen installieren. Der Bitdefender-Sicherheitsagent verwaltet die Sicherheit auf den virtuellen Maschinen. Zudem kommuniziert er mit dem Control Center, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln. Nachdem Sie einen Bitdefender-Sicherheitsagenten in einem Netzwerk installiert haben, wird er alle nicht geschützten virtuellen Maschinen in diesem Netzwerk automatisch erkennen. Security for Virtualized Environments kann dann auf diesen virtuellen Maschinen per Fernzugriff vom Control Center aus installiert werden. Die Remote-Installation erfolgt im Hintergrund, ohne dass der Benutzer dies bemerkt.

In isolierten Netzwerken, die keine direkte Verbindung zur GravityZone-Appliance haben, können Sie den Sicherheitsagenten mit der [Relais-Rolle](#) installieren. In diesem Fall läuft die Kommunikation zwischen der GravityZone-Appliance und den anderen Sicherheitsagenten über den Relais-Agenten, der auch als lokaler Update-Server für die Sicherheitsagenten des isolierten Netzwerks fungiert.



Beachten Sie

Die Maschine, auf der Sie den Relais-Agenten installieren, sollte immer eingeschaltet sein.

⊗ **Warnung**


Vor der Installation sollten Sie bereits installierte Malware-Schutz- und Firewall-Software deinstallieren. Wenn die Bitdefender-Sicherheitssoftware über bestehende Sicherheitssoftware installiert wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen. Windows Defender und die Windows-Firewall werden beim Start der Installation automatisch deaktiviert.

So installieren Sie aus der Ferne Security for Virtualized Environments auf einer oder mehreren virtuellen Maschinen:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
4. Wählen Sie den gewünschten Container im linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

i **Beachten Sie**

Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Maschinen anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

5. Wählen Sie die Entitäten (virtuelle Maschinen, Hosts, Cluster oder Gruppen), auf denen Sie die Sicherheitssoftware installieren möchten.
6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Installieren > BEST**.

Der Assistent **Client installieren** wird angezeigt.

Benutzer	Passwort	Beschreibung	Aktion
<input type="checkbox"/> admin	*****		<input checked="" type="checkbox"/>

Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

7. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:

- **Jetzt** - hiermit startet die Installation sofort.
- **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.



Beachten Sie

Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

8. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
9. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.

**Wichtig**

Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in [diesem Artikel](#).

**Beachten Sie**

Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation von Bitdefender Endpoint Security Tools auf Endpunkten nicht ausgelassen werden.

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

- a. Geben Sie in den entsprechenden Feldern in der Zugangsdaten-Tabellenüberschrift den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

Wenn die Maschinen in einer Domain sind, reicht es aus, die Zugangsdaten des Domain-Administrators einzugeben.

Bei der Eingabe des Namens eines Nutzerkontos Windows-Konvention verwenden:

- Für Active Directory-Maschinen wird folgende Syntax verwendet: `username@domain.com` und `Domäne\Benutzername`. Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).
 - Bei Arbeitsgruppen-Maschinen genügt die Eingabe des Benutzernamens ohne Angabe des Namens der Arbeitsgruppe.
- b. Klicken Sie auf den Button **+Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.

**Beachten Sie**

Die angegebenen Zugangsdaten werden automatisch im [Zugangsdaten-Manager](#) gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben werden müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole klicken.



Wichtig

Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

- c. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.
10. Wählen Sie im Bereich **Installer** die Entität, zu der die Maschinen eine Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.

- **GravityZone-Appliance**, wenn die Maschinen eine direkte Verbindung zur GravityZone-Appliance herstellen.

Hierbei können Sie bei Bedarf auch einen eigenen Kommunikationsserver definieren, indem Sie die entsprechende IP-Adresse bzw. den entsprechenden Hostnamen eingeben.

- **Endpoint-Security-Relais** – wenn Sie die Maschinen mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.



Wichtig

- Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.
- Wenn Sie den Agenten über ein Linux-Relais installieren, müssen die folgenden Voraussetzungen erfüllt sein:
 - Auf dem Relais-Endpunkt muss das Samba-Paket (`smbclient`) mindestens in der Version 4.1.0 sowie der `net-Binary`/Befehl installiert sein, um Windows-Agenten installieren zu können.



Beachten Sie

Der `net-Binary`/Befehl wird üblicherweise mit den Paketen `samba-client` und `/` oder `samba-common` ausgeliefert. Bei einigen Linux-Distributionen (z. B. CentOS 7.4) wird der `net`-Befehl nur bei der Installation der kompletten Samba-Suite

(Common + Client + Server) installiert. Stellen Sie sicher, dass auf Ihrem Relais-Endpunkt der `net`-Befehl verfügbar ist.

- Auf den gewünschten Windows-Endpunkten müssen Administratorfreigabe und Netzwerkfreigabe aktiviert sein.
- Auf den gewünschten Linus- und Mac-Endpunkten muss SSH aktiviert und die Firewall deaktiviert sein.

11. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle Installationspakete, die bisher für Ihr Unternehmen erstellt wurden.

12. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Bearbeitung von Installationspaketen finden Sie in der GravityZone-Installationsanleitung.



Warnung

Bitte beachten Sie, dass das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.


Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.

13. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Client Deinstallieren

So entfernen Sie die Bitdefender-Sicherheitssoftware per Fernzugriff:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der virtuellen Maschinen, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.

5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client deinstallieren**.
6. Ein Konfigurationsfenster wird angezeigt, in dem Sie die folgenden Einstellungen vornehmen können:
 - Wenn Sie möchten, können Sie die Quarantäne-Objekte auf der Client-Maschine belassen.
 - Bei mit vShield integrierten Umgebungen müssen Sie die erforderlichen Zugangsdaten für jede Maschine auswählen, da die Deinstallation sonst fehlschlägt. Wählen Sie **Zugangsdaten für die vShield-Integration verwenden** und markieren Sie dann alle nötigen Zugangsdaten aus der unten angezeigten Zugangsdaten-Manager-Tabelle.
7. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“](#) (S. 214).



Beachten Sie

Wenn Sie den Schutz erneut installieren möchten, müssen Sie den Computer zuerst neu starten.

Update (Aktualisierung)

Überprüfen Sie den Status verwalteter virtueller Maschinen in regelmäßigen Abständen. Wenn Ihnen eine virtuelle Maschine mit Sicherheitsproblemen auffällt, klicken Sie auf ihren Namen, um die Seite **Informationen** anzuzeigen. Weitere Informationen finden Sie unter [„Sicherheitsstatus“](#) (S. 113).

Veraltete Clients oder Sicherheitsinhalten stellen Sicherheitsprobleme dar. In diesen Fällen sollten Sie ein Update auf den entsprechenden virtuellen Maschinen durchführen. Diese Aufgabe kann lokal von der virtuellen Maschine aus oder per Fernzugriff vom Control Center aus durchgeführt werden.

So können Sie den Client und die Sicherheitsinhalte auf verwalteten virtuellen Maschinen per Fernzugriff aktualisieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).

3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der virtuellen Maschinen, auf denen Sie ein Client-Update durchführen möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Update**. Ein Konfigurationsfenster wird sich öffnen.
6. Sie können nur das Produkt, nur die Sicherheitsinhalte oder beides aktualisieren.
7. Bei Linux-Betriebssystemen und mit vShield integrierten Maschinen müssen die nötigen Zugangsdaten ebenfalls ausgewählt werden. Markieren Sie **Zugangsdaten für Linux und die vShield-Integration verwenden** und wählen Sie dann die nötigen Zugangsdaten aus der unten angezeigten Zugangsdaten-Manager-Tabelle.
8. Klicken Sie auf **Update**, um die Aufgabe auszuführen. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Client neu konfigurieren

Die Module, Rollen und Scan-Modi des Sicherheitsagenten sind zunächst im Installationspaket konfiguriert. Nach der Installation des Sicherheitsagenten in Ihrem Netzwerk können Sie die anfänglichen Einstellungen jederzeit ändern, indem Sie per Fernzugriff einer Aufgabe **Client neu konfigurieren** an die gewünschten verwalteten Endpunkte senden.

Warnung

Bitte beachten Sie, dass die Aufgabe **Client neu konfigurieren** alle Installationseinstellungen überschreibt. Keine der ursprünglich Einstellungen wird beibehalten. Achten Sie bei der Verwendung dieser Aufgabe darauf, alle Installationseinstellungen für die gewünschten Endpunkte neu zu konfigurieren.

So ändern Sie die Installationseinstellungen für eine oder mehrere virtuelle Maschinen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).

3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der virtuellen Maschinen, bei denen Sie die Installationseinstellungen ändern möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client neu konfigurieren**.
6. Konfigurieren Sie im Bereich **Allgemein** den Zeitpunkt, zu dem die Aufgabe ausgeführt werden soll:
 - **Jetzt** - hiermit startet die Aufgabe sofort.
 - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Aufgabe fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.



Beachten Sie

Wenn zum Beispiel andere wichtige Prozesse ebenfalls auf der Maschine ausgeführt werden müssen, können Sie die Aufgabe so planen, dass sie alle 2 Stunden ausgeführt wird. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis sie erfolgreich abgeschlossen wird.

7. Konfigurieren Sie die Module, Rollen und Scan-Modi für die gewünschten Endpunkte nach Bedarf. Weitere Informationen hierzu finden Sie in der GravityZone-Installationsanleitung.



Warnung

- Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden.
Bitte beachten Sie, dass das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.
 - Bitdefender Tools (Vorängeragent) unterstützt nur den zentralisierten Scan.
8. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.
Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [„Aufgaben anzeigen und verwalten“](#) (S. 214).

Netzwerkerkennung


Die Netzwerkerkennung wird automatisch nur von Sicherheitsagenten mit [Relais-Rolle](#) durchgeführt. Wenn Sie in Ihrem Netzwerk keinen Relais-Agenten installiert haben, müssen Sie manuell eine Netzwerkerkennungsaufgabe von einem geschützten Endpunkt aus senden.

So führen Sie eine Netzwerkerkennungsaufgabe in Ihrem Netzwerk durch:



Wichtig


Wenn Sie mit einem Linux-Relais andere Linux- oder Mac-Endpunkte erkennen möchten, müssen Sie entweder auf den Zielendpunkten Samba installieren oder sie in einem Active Directory zusammenfassen und DHCP verwenden. Damit wird NetBIOS automatisch auf ihnen konfiguriert.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen der Maschine, über die Sie eine Netzwerkerkennung durchführen möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Netzwerkerkennung**.
6. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.
Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Anwendungserkennung

So können Sie die Anwendungen in Ihrem Netzwerk ermitteln:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle virtuellen Maschinen des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.

4. Wählen Sie die virtuellen Maschinen aus, auf denen die Anwendungen ermittelt werden sollen.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Anwendungserkennung** aus.

**Beachten Sie**

Auf den ausgewählten virtuellen Maschinen muss Bitdefender Endpoint Security Tools mit Anwendungssteuerung installiert und aktiviert sein. Andernfalls wird die Aufgabe ausgegraut. Wenn eine ausgewählte Gruppe sowohl gültige als auch ungültige Ziele enthält, wird die Aufgabe nur an die gültigen Endpunkte übermittelt.

6. Klicken Sie zum Fortsetzen des Vorgangs im Bestätigungsfenster auf **Ja**.

Die ermittelten Anwendungen und Prozesse werden auf der Seite **Netzwerk- > Anwendungsbestand** angezeigt. Weitere Informationen finden Sie unter „Anwendungsbestand“ (S. 199).

**Beachten Sie**

Die Aufgabe **Anwendungserkennung** kann je nach Anzahl der installierten Anwendungen einige Zeit in Anspruch nehmen. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „Aufgaben anzeigen und verwalten“ (S. 214).


Computer neu starten

Sie können verwaltete virtuelle Maschinen aus der Ferne neu starten.

**Beachten Sie**

Bevor Sie einzelne virtuelle Maschinen neu starten, sollten Sie einen Blick auf die Seite **Netzwerk > Aufgaben** werfen. Zuvor erstellte Aufgaben könnten derzeit noch auf den Maschinen laufen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der **Ansichtsauswahl**.
3. Wählen Sie den gewünschten Container im linken Fenster. Alle Entitäten des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie die Kästchen der virtuellen Maschinen, die Sie neu starten möchten.

5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Computer neu starten**.
6. Wählen Sie den Zeitpunkt des Neustarts:
 - Wählen Sie **Jetzt neu starten**, um die virtuellen Maschinen sofort neu zu starten.
 - Wählen Sie **Neustart am**, und nutzen Sie die Eingabefelder weiter unten, um den Neustart für einen bestimmten Zeitpunkt zu planen.
7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.
Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter [Aufgaben anzeigen und verwalten](#).

Security Server installieren

So installieren Sie Security Server in Ihrer virtuellen Umgebung:

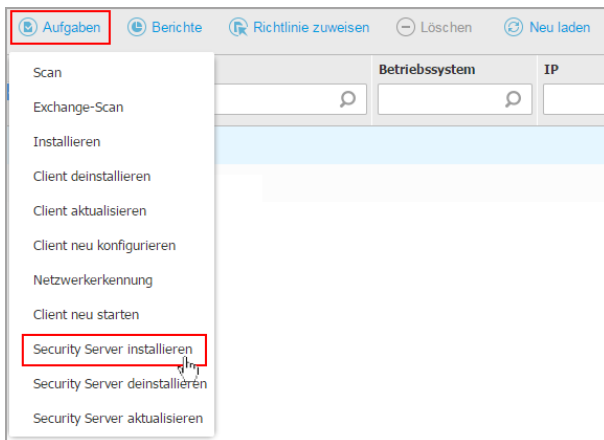
1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Durchsuchen Sie das Nutanix-, VMware- oder Citrix-Inventar und markieren Sie die Kästchen der gewünschten Hosts oder Container (Nutanix Prism, vCenter Server, XenServer oder Rechenzentrum). Um Zeit zu sparen, können Sie auch direkt den Root-Container auswählen wählen (Nutanix-Inventar, VMware-Inventar oder Citrix-Inventar). Im Installationsassistenten können Sie Hosts einzeln auswählen.



Beachten Sie

Sie können nicht Hosts von verschiedenen Ordnern gleichzeitig auswählen.

4. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle und wählen Sie **Security Server installieren** aus dem Menü. Das Fenster **Security Server-Installation** wird angezeigt.



Installieren von Security Server über das Aufgabenmenü

- Alle im ausgewählten Container gefundenen Hosts werden in der Liste aufgeführt. Wählen Sie den Host, auf dem Sie die Security Server-Instanzen installieren möchten.
- Wählen Sie die gewünschten Konfigurationseinstellungen.



Wichtig

Wenn Sie bei der gleichzeitigen Installation mehrerer Instanzen von Security Server gemeinsame Einstellungen verwenden möchten, müssen die Hosts denselben Speicher benutzen, per DHCP-Server zugewiesene IP-Adressen haben und Teil desselben Netzwerks sein.

- Klicken Sie auf **Weiter**.
- Geben Sie die entsprechenden VMware-vShield-Zugangsdaten für jede vCenter-Maschine an.
- Geben Sie einen aussagekräftigen Namen für den Security Server ein.
- Wählen Sie in VMware-Umgebungen aus dem Menü **Container installieren** den Container, in dem Sie den Security Server installieren möchten.
- Wählen Sie den Ziel-Speicherort.
- Wählen Sie die Art der Speicherzuweisung. Für die Installation der Appliance wird die klassische Speicherzuweisung empfohlen.

**Wichtig**

Wenn bei Verwendung der schlanken Speicherzuweisung der Speicherplatz knapp wird, hängt sich die Security Server auf, wodurch der Host nicht mehr geschützt ist.

13. Konfigurieren Sie die Speicher- und CPU-Ressourcenzuteilung je nach VM-Konsolidierungsrate auf dem Host. Wählen Sie **Gering**, **Mittel** oder **Hoch**, um die empfohlenen Einstellungen für die Ressourcenzuteilung zu laden, oder **Manuell**, um die Ressourcenzuteilung manuell zu konfigurieren.
14. Vergeben Sie ein Administrator-Passwort für die Security Server-Konsole. Wenn Sie ein Administratorpasswort festlegen, setzt dieses das Standard-Root-Passwort ("sve") außer Kraft.
15. Legen Sie die Zeitzone der Appliance fest.
16. Wählen Sie die Netzwerkkonfigurationsart für das Bitdefender-Netzwerk. Die IP-Adresse des Security Server darf im Laufe der Zeit nicht geändert werden, da sie von Linux-Agenten zur Kommunikation verwendet wird.
Wenn Sie DHCP wählen, konfigurieren Sie den DHCP-Server so, dass er eine IP-Adresse für die Appliance reserviert.
Wenn Sie die Option "statisch" wählen, müssen Sie IP-Adresse, Subnetz-Maske, Gateway und DNS eingeben.
17. Wählen Sie das vShield-Netzwerk und geben Sie die vShield-Zugangsdaten ein. Die Standardbezeichnung für das vShield-Netzwerk `vm-service-vshield-pg`.
18. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

**Wichtig**


- Die Pakete mit Security Server sind standardmäßig nicht in der GravityZone-Appliance enthalten. Je nach den Einstellungen, die der Root-Administrator vorgenommen hat, wird das Paket mit Security Server entweder heruntergeladen, wenn eine Installationsaufgabe für Security Server gestartet wird. Falls nicht, wird der Administrator über das fehlende Image informiert und die Installation angehalten. Wenn das Paket fehlt, muss der Root-Administrator es manuell herunterladen, um die Installation erfolgreich durchzuführen.
- In Nutanix-Umgebungen kann die Installation des Security Servers per Fernzugriff aus verschiedenen Gründen fehlschlagen, so z. B. wenn der Prism

Element-Cluster in Prism Central registriert ist. In solchen Fällen empfiehlt es sich, die Installation des Security Servers manuell durchzuführen. Weitere Einzelheiten finden Sie in diesem [Artikel in der Wissensdatenbank](#).

19. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Security Server deinstallieren

So deinstallieren Sie einen Security Server:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie das Rechenzentrum oder den Ordner, in dem sich der Host, auf dem Security Server installiert ist, befindet.
4. Markieren Sie das Kästchen des Hosts, auf dem der Security Server installiert ist.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Security Server deinstallieren**.
6. Geben Sie die vShield-Zugangsdaten ein und klicken Sie auf **Ja**, um die Aufgabe zu erstellen.
7. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Security Server aktualisieren

So aktualisieren Sie einen Security Server:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den Host, auf dem Security Server installiert ist.

Den Security Server finden Sie leicht über das [Filter](#)menü. Gehen Sie dazu wie folgt vor:

- Gehen Sie zum Reiter **Sicherheit** und wählen Sie nur **Security Servers** aus.


- Gehen Sie zum Reiter **Tiefe** und wählen Sie **Alle Objekte rekursiv**.



Beachten Sie

Falls Sie ein Virtualisierungsverwaltungstool verwenden, das derzeit nicht mit dem Control Center integriert ist, wird der Security Server unter **Benutzerdefinierte Gruppen** eingeordnet.

Weitere Informationen zu unterstützten Virtualisierungsplattformen finden Sie in der GravityZone-Installationsanleitung.

4. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Security Server aktualisieren**.
5. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.
6. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).



Wichtig

Diese Methode wird für Updates von Security Server for NSX empfohlen, da andernfalls die auf der Appliance gespeicherte Quarantäne verloren gehen würde.

HVI-Ergänzungspaket installieren

Um virtuelle Maschinen über HVI zu schützen, muss das Ergänzungspaket auf dem Host installiert sein. Dieses Paket dient dazu, die Kommunikation zwischen dem Hypervisor und dem auf dem Host installierten Security Server sicherzustellen. Nach der Installation schützt HVI die virtuellen Maschinen, in deren Richtlinie HVI aktiviert ist.



Wichtig

- HVI schützt virtuelle Maschinen ausschließlich auf Citrix Xen -Hypervisoren.
- Der bestehende Sicherheitsagent der virtuellen Maschine muss nicht deinstalliert werden.

Installation des Ergänzungspakets auf dem Host:

1. Gehen Sie zur Seite **Konfiguration > Update**.
2. Wählen Sie das HVI-Ergänzungspaket in der Liste **Komponenten** aus und klicken Sie das Feld **Download** oben in der Tabelle an.

3. Gehen Sie zur Seite **Netzwerk** und wählen Sie in der Auswahlliste **Virtuelle Maschinen**.
4. Wählen Sie nun im Menu **Ansichten** auf der linken Seite **Server** aus.
5. Wählen Sie einen oder mehrere Xen-Hosts aus dem Netzwerkinventar. Sie können die verfügbaren Hosts ganz einfach über die Option **Typ > Hosts** im Menu **Filter** anzeigen.
6. Klicken Sie das Feld **Aufgaben** auf der rechten Seite an und wählen Sie **HVI Ergänzungspaket installieren**. Das Installationsfenster öffnet sich.
7. Entscheiden Sie, wann die Installation durchgeführt werden soll. Sie können die Installation direkt nach dem Speichern der Aufgabe oder zu einem späteren Zeitpunkt durchführen. Falls die Installation zu der festgelegten Zeit nicht vollständig durchgeführt werden kann, wird der Vorgang automatisch den Einstellungen entsprechend wiederholt. Falls Sie zum Beispiel mehrere Hosts ausgewählt haben und ein Host zum festgelegten Installationszeitpunkt nicht verfügbar ist, wird die Aufgabe zum festgelegten Zeitpunkt wiederholt.
8. Die Übernahme der Änderungen und Abschluss der Installation erfordert einen Neustart des Hosts. Falls der Host unbeaufsichtigt neu starten soll, wählen Sie **Autom. Neustart (falls erforderlich)**.
9. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.
Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

HVI-Ergänzungspaket deinstallieren

So können Sie das Ergänzungspaket von den Hosts deinstallieren:

1. Gehen Sie zur Seite **Netzwerk** und wählen Sie in der Auswahlliste **Virtuelle Maschinen**.
2. Wählen Sie nun im Menu **Ansichten** auf der linken Seite **Server** aus.
3. Wählen Sie einen oder mehrere Xen-Hosts aus dem Netzwerkinventar. Sie können die verfügbaren Hosts ganz einfach über die Option **Typ > Hosts** im Menu **Filter** anzeigen.
4. Klicken Sie das Feld **Aufgaben** auf der rechten Seite an und wählen Sie **HVI-Ergänzungspaket desinstallieren**. Das Konfigurationsfenster wird angezeigt.

5. Planen Sie einen Zeitpunkt für die Entfernung des Pakets. Sie können die Installation direkt nach dem Speichern der Aufgabe oder zu einem späteren Zeitpunkt durchführen. Falls die Entfernung zum festgelegten Zeitpunkt nicht vollständig durchgeführt werden kann, wird der Vorgang automatisch den Einstellungen entsprechend wiederholt. Falls Sie zum Beispiel mehrere Hosts ausgewählt haben und ein Host zum Zeitpunkt der Entfernung nicht verfügbar ist, wird die Aufgabe zum festgelegten Zeitpunkt wiederholt.
6. Der Host muss zum Abschluss der Entfernung neu gestartet werden. Falls der Host unbeaufsichtigt neu starten soll, wählen Sie **Autom. Neustart (falls erforderlich)**.
7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.
Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

HVI-Ergänzungspaket aktualisieren

So können Sie das Ergänzungspaket auf den Hosts aktualisieren:

1. Installieren Sie das neueste verfügbare HVI-Ergänzungspaket.
Weitere Informationen finden Sie unter „[HVI-Ergänzungspaket installieren](#)“ (S. 164).
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Virtuelle Maschinen** aus der Ansichtsauswahl.
4. Wählen Sie nun im Menu **Ansichten** auf der linken Seite **Server** aus.
5. Wählen Sie einen oder mehrere Xen-Hosts aus dem Netzwerkinventar.
Sie können die verfügbaren Hosts ganz einfach über die Option **Typ > Hosts** im Menu **Filter** anzeigen.
6. Klicken Sie auf die **Aufgaben**-Schaltfläche auf der rechten Seite und wählen Sie **HVI-Ergänzungspaket aktualisieren**. Das Konfigurationsfenster wird angezeigt.
7. Planen Sie einen Zeitpunkt für die Aktualisierung des Pakets. Sie können die Installation direkt nach dem Speichern der Aufgabe oder zu einem späteren Zeitpunkt durchführen.

Falls das Update zum festgelegten Zeitpunkt nicht vollständig durchgeführt werden kann, wird der Vorgang automatisch den Einstellungen entsprechend wiederholt. Falls Sie zum Beispiel mehrere Hosts ausgewählt haben und ein


Host zum festgelegten Update-Zeitpunkt nicht verfügbar ist, wird die Aufgabe zum festgelegten Zeitpunkt wiederholt.

8. Wählen Sie **Autom. Neustart (falls erforderlich)**, wenn Sie den Host unbeaufsichtigt neu starten möchten. Andernfalls müssen Sie den Host manuell neu starten, um das Update anzuwenden.
9. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie den Aufgabenstatus überwachen.

Benutzerdefiniertes Tool injizieren

Gehen Sie folgendermaßen vor, um Tools in Ziel-Gastbetriebssystemen zu injizieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Wählen Sie die Kästchen für die Zielendpunkte aus.
5. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Benutzerdefiniertes Tool injizieren**. Ein Konfigurationsfenster wird geöffnet.
6. Wählen Sie aus dem Klappmenü alle zu injizierenden Tools aus. Für jedes Tool wird ein reduzierbarer Bereich mit den entsprechenden Einstellungen angezeigt. Diese Tools wurden zuvor in GravityZone hochgeladen. Wenn das gesuchte Tool in der Liste nicht aufgeführt ist, rufen Sie das **Tool-Verwaltungszentrum** auf und fügen Sie es von dort aus hinzu. Weitere Informationen finden Sie unter [„Benutzerdefiniert Tool-Injektion mit HVI“ \(S. 511\)](#).
7. Gehen Sie für jedes im Fenster angezeigt Tool folgendermaßen vor:
 - a. Klicken Sie auf den Namen des Tools, um den entsprechenden Bereich anzuzeigen oder zu verbergen.
 - b. Geben Sie die Befehlszeile des Tools gemeinsam mit allen benötigten Eingabeparametern ein, so wie Sie es auch in der Eingabeaufforderung bzw. im Terminal tun würden. Zum Beispiel:


```
bash script.sh <param1> <param2>
```


Für die BD-Bereinigungstools können Sie aus den beiden Klappmenüs nur die Bereinigungsaktion sowie die Ersatzaktion zur Bereinigung auswählen.

- c. Verweisen Sie auf den Speicherort, von dem der Security Server die Protokolle abrufen soll:
 - **stdout**. Markieren Sie das Kästchen, um die Protokolle über den Standard-Ausgangsübertragungskanal abzurufen.
 - **Ausgabedatei**. Markieren Sie dieses Kästchen, um auf dem Endpunkt gespeicherte Protokolldateien abzurufen. In diesem Fall müssen Sie den Pfad eingeben, über den der Security Server die Datei finden kann. Sie können sowohl absolute Pfade als auch Systemvariablen eingeben.
Hier eine weitere Option: **Protokolldateien nach der Übermittlung vom Gast löschen**. Wählen Sie diese Option, wenn die Dateien auf dem Endpunkt nicht mehr benötigt werden.
8. Wenn Sie die Protokolldateien vom Security Server zu einem anderen Speicherort verschieben möchten, müssen Sie den Pfad zum Zielspeicherort und die Anmeldeinformationen für die Authentifizierung angeben.
9. Gelegentlich braucht das Tool unter Umständen länger als erwartet, um den Auftrag abzuschließen, oder reagiert nicht mehr. Um in diesen Fällen Abstürze zu verhindern, können Sie im Bereich **Sicherheitskonfiguration** festlegen, nach wie vielen Stunden der Security Server den Tool-Prozess automatisch beenden soll.
10. Klicken Sie auf **Speichern**.
Auf der Seite **Aufgaben** können Sie den Aufgabenstatus einsehen. Weitere Details finden Sie zudem im **HVI-Drittanbieter-Injektionsstatus-Bericht**.

6.3.6. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte auf verwalteten virtuellen Maschinen erstellen:


1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).

3. Wählen Sie den gewünschten Container im linken Fenster. Alle virtuellen Maschinen des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Filtern Sie den Inhalt der ausgewählten Gruppe nur nach verwalteten virtuellen Maschinen.
5. Markieren Sie die Kästchen für die virtuellen Maschinen, die Sie in den Bericht aufnehmen möchten.
6. Klicken Sie auf die Schaltfläche  **Bericht** am oberen Rand der Tabelle, und wählen Sie den Berichtstyp aus dem Menü. Weitere Informationen finden Sie unter „[Berichte zu Computern und virtuellen Maschinen](#)“ (S. 439).
7. Konfigurieren Sie die Berichtsoptionen. Weitere Informationen finden Sie unter „[Berichte erstellen](#)“ (S. 459)
8. Klicken Sie auf **Generieren**. Der Bericht wird sofort angezeigt. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von der Anzahl der ausgewählten virtuellen Maschinen ab.

6.3.7. Richtlinien zuweisen

Über [Richtlinien](#) können Sie Sicherheitseinstellungen auf virtuellen Maschinen verwalten.

Auf der Seite **Netzwerk** können Sie Richtlinien für jede virtuelle Maschine bzw. Gruppe von virtuellen Maschinen anzeigen, ändern und zuweisen.

 **Beachten Sie** Sicherheitseinstellungen stehen nur für verwaltete virtuelle Maschinen zur Verfügung. Zur vereinfachten Anzeige und Verwaltung früherer Sicherheitseinstellungen kann man das Netzwerkinventar nur durch verwaltete virtuelle Maschinen [Filtern](#).


So zeigen Sie die Sicherheitseinstellungen an, die einer bestimmten virtuellen Maschine zugewiesen wurden:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle virtuellen Maschinen des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.

4. Klicken Sie auf den Namen der gewünschten virtuellen Maschine. Es öffnet sich ein Informationsfenster.
5. Klicken Sie im Reiter **Allgemein** des Bereichs **Richtlinie** auf den Namen der aktuellen Richtlinie, um ihre Einstellungen anzuzeigen.
6. Sie können die Sicherheitseinstellungen nach Bedarf ändern, sofern der Richtlinienersteller Änderungen an dieser Richtlinie durch andere Benutzer erlaubt hat. Bitte beachten Sie, dass Ihre Änderungen sich auch auf alle anderen virtuellen Maschinen auswirken, denen diese Richtlinie zugewiesen wurde.

Weitere Informationen zur Richtlinieneinstellungen für virtuelle Maschinen finden Sie unter „[Sicherheitsrichtlinien](#)“ (S. 227)


So weisen Sie einer virtuellen Maschine oder einer Gruppe von virtuellen Maschinen eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Virtuelle Maschinen** aus der [Ansichtsauswahl](#).
3. Wählen Sie den gewünschten Container im linken Fenster. Alle virtuellen Maschinen des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
4. Markieren Sie das Kästchen der gewünschten Entität. Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
5. Klicken Sie auf die Schaltfläche  **Richtlinie zuweisen** am oberen Ende der Tabelle.
6. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor.

Weitere Informationen finden Sie unter „[Richtlinien zuweisen](#)“ (S. 231).




Warnung

Bei Richtlinien mit aktiviertem Hypervisor Memory Introspection müssen die Zielmaschinen unter Umständen direkt nach der Richtlinienzuweisung neu gestartet werden. Maschinen, für die dies zutrifft, werden unter **Netzwerk** mit dem Symbol  **Neustart steht aus** gekennzeichnet.

6.3.8. Der Wiederherstellungsmanager für verschlüsselte Laufwerke

Wenn Endpunkt-Benutzer ihr Verschlüsselungspasswort vergessen und somit nicht mehr auf verschlüsselte Laufwerke ihres Computers zugreifen können, können Sie ihnen mit Wiederherstellungsschlüsseln von der Seite **Netzwerk** helfen.

So rufen Sie einen Wiederherstellungsschlüssel ab:

1. Gehen Sie zur Seite **Netzwerk**.
2. Klicken Sie in der Symbolleiste des linken Fensters auf die Schaltfläche  **Wiederherstellungsmanager**. Ein neues Fenster wird angezeigt.
3. Geben Sie im Bereich **Bezeichner** des Fensters die folgenden Daten ein:

- a. Die Wiederherstellungsschlüssel-ID des verschlüsselten Laufwerks. Die Wiederherstellungsschlüssel-ID ist eine Folge von Buchstaben und Zahlen, die im BitLocker-Wiederherstellungsfenster auf dem Endpunkt einsehbar ist.

Unter Windows ist die Wiederherstellungsschlüssel-ID eine Folge von Buchstaben und Zahlen, die im BitLocker-Wiederherstellungsfenster auf dem Endpunkt einsehbar ist.

Alternativ können Sie die Option **Wiederherstellung** im Reiter **Schutz** der [Details virtueller Maschinen](#) wählen, um die Wiederherstellungsschlüssel-ID automatisch einzufügen. Das funktioniert sowohl unter Windows als auch unter macOS.

- b. Das Passwort Ihres GravityZone-Kontos.
4. Klicken Sie auf **Anzeigen**. Das Fenster wird vergrößert.

Unter **Laufwerksinformationen** werden die folgenden Daten aufgeführt:

- a. Name des Laufwerks
 - b. Laufwerktyp (bootfähig oder nicht bootfähig).
 - c. Endpunkt-Name (wie im Netzwerkinventar aufgeführt)
 - d. Wiederherstellungsschlüssel. Unter Windows ist der Wiederherstellungsschlüssel ein Passwort, das bei der Verschlüsselung des Laufwerks automatisch generiert wird. Unter macOS ist der Wiederherstellungsschlüssel das Passwort des Benutzerkontos.
5. Schicken Sie dem Endpunkt-Benutzer den Wiederherstellungsschlüssel.

Details zur Verschlüsselung und Entschlüsselung von Laufwerken mit GravityZone finden Sie hier: „[Verschlüsseln](#)“ (S. 401).

6.3.9. Freigeben von Lizenzplätzen

In Active Directory-, vCenter Server- (ohne vShield, NSX oder HVI) und Xen Server-Inventaren können Sie, ohne das Deinstallationsprogramm auszuführen, problemlos die Lizenzplätze von virtuellen Maschinen freigeben, bei denen der Sicherheitsagent entfernt wurde.

Anschließend werden die Zielmaschinen im Netzwerkinventar nicht mehr verwaltet.

So geben Sie einen Lizenzplatz frei:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie in der **Ansichtsauswahl** einen der Einträge **Computer und virtuelle Maschinen** oder **Virtuelle Maschinen**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. In der rechten Tabelle werden alle virtuellen Maschinen angezeigt.
4. Wählen Sie die virtuelle Maschine aus, deren Lizenz Sie freigeben möchten.
5. Klicken Sie auf **⊖ Lizenz löschen** oben in der Tabelle.
6. Klicken Sie zum Fortsetzen des Vorgangs im Bestätigungsfenster auf **Ja**.

6.4. Mobilgeräte

Um die Sicherheit der in Ihrem Unternehmen verwendeten Mobilgeräte zu verwalten, müssen Sie die Geräte zunächst in der Control Center bestimmten Benutzern zuordnen und dann die GravityZone Mobile Client-Anwendung auf jedem Gerät installieren und aktivieren.

Die Mobilgeräte können dabei Eigentum des Unternehmens oder der Benutzer selbst sein. Sie können GravityZone Mobile Client auf den Mobilgeräten installieren und aktivieren und sie dann den jeweiligen Benutzern zur Verfügung stellen. Die Benutzer können GravityZone Mobile Client auch selbst installieren und aktivieren, indem sie den Anweisungen folgen, die sie per E-Mail erhalten haben. Weitere Informationen hierzu finden Sie in der GravityZone-Installationsanleitung.

Sie können die Mobilgeräte der Benutzer in Ihrem Konto anzeigen, indem Sie zum Bereich **Netzwerk** gehen und **Mobilgeräte** aus der **Dienstauswahl** auswählen. Auf der Seite **Netzwerk** werden die verfügbaren Benutzergruppen im linken Fenster und die entsprechenden Benutzer und Geräte im rechten Fenster angezeigt.

Wenn die Integration mit Active Directory konfiguriert wurde, können Sie Mobilgeräte bestehenden Active-Directory-Benutzern zuordnen. Sie können auch unter **Benutzerdefinierte Gruppen** Benutzer erstellen und ihnen Mobilgeräte hinzufügen.

Über den Reiter **Ansichten** im **Filtermenü** am oberen Rand der Tabelle können Sie im rechten Fenster zur Ansicht **Benutzer** oder **Geräte** wechseln. In der Ansicht **Benutzer** können Sie Benutzer im Control Center verwalten (Benutzer und Mobilgeräte hinzufügen, Anzahl der Geräte pro Benutzer überprüfen, usw.). In der Ansicht **Geräte** können Sie Einzelheiten zu jedem Mobilgeräte im Control Center einsehen und verwalten.

Im Control Center haben Sie folgende Möglichkeiten zur Verwaltung von Benutzern und Mobilgeräten:

- [Benutzerdefinierte Benutzer hinzufügen](#)
- [Benutzern Mobilgeräte hinzufügen](#)
- [Benutzerdefinierte Benutzer in Gruppen organisieren](#)
- [Benutzer und Geräte filtern und suchen](#)
- [Status und Details von Benutzern und Geräten überprüfen](#)
- [Aufgaben auf Mobilgeräten ausführen](#)
- [Schnellberichte zu Mobilgeräten erstellen](#)
- [Sicherheitseinstellungen von Geräten anzeigen und ändern](#)
- [Das Inventar des Control Center mit dem von Active Directory synchronisieren](#)
- [Benutzer und Mobilgeräte löschen](#)

6.4.1. Benutzerdefinierte Benutzer hinzufügen

Wenn die Integration mit Active Directory konfiguriert wurde, können Sie Mobilgeräte bestehenden Active-Directory-Benutzern zuordnen.

In Situationen ohne Active Directory müssen Sie zunächst benutzerdefinierte Benutzer erstellen, um eine Möglichkeit zu haben, die Eigentümer von Mobilgeräten zu identifizieren.

Benutzerdefinierte Benutzer können auf zwei unterschiedliche Arten erstellt werden. Sie können Sie entweder einzelnen hinzufügen oder eine CSV-Datei importieren.

So fügen Sie einen benutzerdefinierten Benutzer hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der **Dienstauswahl**.

3. Klicken Sie am oberen Rand der Tabelle auf das Menü **Filter** und wechseln Sie dann zum Reiter **Ansicht**. Vergewissern Sie sich, dass die Option **Benutzer** aktiviert ist.
4. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**.
5. Klicken Sie auf die Schaltfläche **Benutzer hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
6. Geben Sie die Informationen des gewünschten Benutzers an:
 - Einen aussagekräftigen Benutzernamen (z. B. den vollen Namen des Benutzers)
 - Die E-Mail-Adresse des Benutzers



Wichtig

- Vergewissern Sie sich, dass die E-Mail-Adresse gültig ist. Wenn Sie ein Gerät hinzufügen, erhält der Benutzer eine E-Mail mit den Installationsanweisungen.
- Jede E-Mail-Adresse kann nur zu einem Benutzer gehören.

7. Klicken Sie auf **OK**.

So importieren Sie Mobilgerät-Benutzer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Dienstauswahl](#).
3. Klicken Sie am oberen Rand der Tabelle auf das Menü **Filter** und wechseln Sie dann zum Reiter **Ansicht**. Vergewissern Sie sich, dass die Option **Benutzer** aktiviert ist.
4. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**.
5. Klicken Sie auf **Benutzer importieren**. Ein neues Fenster wird geöffnet.
6. Wählen Sie die CSV-Datei aus und klicken Sie auf **Wiederherstellen**. Das Fenster wird geschlossen und die Tabelle mit den importierten Benutzern gefüllt.



Beachten Sie

Wenn ein Fehler auftritt, wird eine Meldung angezeigt und die Tabelle nur mit den gültigen Benutzern gefüllt. Bestehende Benutzer werden übersprungen.

Später können Sie unter **Benutzerdefinierte Gruppen** [Benutzergruppen erstellen](#) .

Die einem Benutzer zugewiesenen Richtlinie und Aufgaben gelten für alle Geräte dieses Benutzers.

6.4.2. Benutzern Mobilgeräte hinzufügen

Jeder Benutzer kann beliebig viele Mobilgeräte haben. Sie können Geräte einem oder mehreren Benutzern hinzufügen, aber immer nur ein Gerät pro Benutzer gleichzeitig.

Ein Gerät einem einzelnen Benutzer hinzufügen

So fügen Sie einem Benutzer ein Gerät hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Finden Sie den Benutzer in den **Active-Directory**-Gruppen oder in den **benutzerdefinierten Gruppen** und markieren Sie das entsprechende Kästchen im rechten Fenster.



Beachten Sie

Im Reiter **Ansicht** müssen die **Filter** auf **Benutzer** eingestellt sein.

4. Klicken Sie auf die Schaltfläche  **Gerät hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.

Gerät hinzufügen

Gerätename:

Name automatisch konfigurieren

Eigentümer:

Aktivierungszugangsdaten anzeigen

OK Abbrechen

Ein Mobilgerät für einen Benutzer hinzufügen

5. Konfigurieren Sie die Details des Mobilgeräts:
 - a. Geben Sie einen aussagekräftigen Namen für das Gerät ein.

- b. Mit der Option **Name automatisch konfigurieren** wird der Geräte name automatisch generiert. Nach dem Hinzufügen erhält das Gerät einen generierten Namen. Sobald das Gerät aktiviert ist, wird es automatisch mithilfe der entsprechenden Hersteller- und Modell-Informationen umbenannt.
 - c. Wählen Sie den Eigentübertyp des Geräts (geschäftlich/enterprise oder privat). Sie können Mobilgeräte jederzeit nach Eigentübertyp filtern und nach Ihren Wünschen verwalten.
 - d. Wählen Sie die Option **Aktivierungszugangsdaten anzeigen**, wenn Sie den GravityZone Mobile Client auf dem Gerät des Benutzers installieren möchten.
6. Klicken Sie auf **OK**, um das Gerät hinzuzufügen. Es wird sofort eine E-Mail an den Benutzer gesendet, die Installationsanweisungen und Aktivierungsdetails für das Gerät enthält. Die Aktivierungsdetails enthalten das Aktivierungs-Token und die Adresse des Kommunikationsservers (und den entsprechenden QR-Code).
7. Wenn Sie die Option **Aktivierungszugangsdaten anzeigen** ausgewählt haben, wird das Fenster **Aktivierungsdetails** mit dem einzigartigen Aktivierungs-Token, der Adresse des Kommunikationsservers und dem entsprechenden QR-Code angezeigt.



Aktivierungsdetails

Aktivierungs-Token: 1846917580

Server-URL: 10.10.17.80:8443

QR-Code

Schließen

Informationen zur Aktivierung von Mobilgeräten

Wenn Sie nach der GravityZone Mobile Client-Installation aufgefordert werden, das Gerät zu aktivieren, geben Sie das Aktivierungs-Token und die Adresse des Kommunikationsservers ein oder scannen Sie den bereitgestellten QR-Code.

Geräte mehreren Benutzern hinzufügen

So fügen Sie einer Auswahl an Benutzern und Gruppen Mobilgeräte hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Finden Sie die Benutzer oder Gruppen in den **Active-Directory**-Ordnern oder in den **benutzerdefinierten Gruppen** und markieren Sie die entsprechenden Kästchen im rechten Fenster.



Beachten Sie

Im Reiter **Ansicht** müssen die **Filter** auf **Benutzer** eingestellt sein.

4. Klicken Sie auf die Schaltfläche **Gerät hinzufügen** auf der rechten Seite der Tabelle. In diesem Fall können Sie im Konfigurationsfenster nur den Eigentümer des Geräts definieren.

Wenn es Benutzer gibt, die keine E-Mail-Adresse haben, werden Sie mit einer Meldung darauf hingewiesen. Die Liste der entsprechenden Benutzer kann im Bereich **Benachrichtigung** des Control Center eingesehen werden.

Mobilgeräte, die durch eine Mehrfachauswahl erstellt wurden, erhalten standardmäßig einen generischen Namen im Control Center. Sobald ein Gerät aktiviert ist, wird es automatisch mithilfe der entsprechenden Hersteller- und Modell-Informationen umbenannt.

5. Klicken Sie auf **OK**, um die Geräte hinzuzufügen. Es wird sofort eine E-Mail an jeden Benutzer gesendet, die Installationsanweisungen und Aktivierungsdetails für das Gerät enthält. Die Aktivierungsdetails enthalten das Aktivierungs-Token und die Adresse des Kommunikationsservers (und den entsprechenden QR-Code).

Im rechten Fenster können Sie in der Spalte **Geräte** sehen, wie viele Geräte jedem Benutzer zugeordnet wurden.

6.4.3. Benutzerdefinierte Benutzer in Gruppen organisieren

Sie können die verfügbaren Benutzergruppen im linken Fenster der Seite **Netzwerk** einsehen.

Active-Directory-Benutzer finden Sie unter **Active Directory**. Die Active-Directory-Gruppen können Sie nicht bearbeiten. Sie können diesen Benutzern nur Geräte hinzufügen bzw. die zugeordneten Geräte anzeigen lassen.

Sie können alle Benutzer außerhalb des Active Directory unter **Benutzerdefinierte Gruppen** sortieren. Dort können Sie nach Belieben Gruppen erstellen und organisieren. Ein großer Vorteil ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Unter **Benutzerdefinierte Gruppen** können Sie Benutzergruppen innerhalb einer benutzerdefinierten Baumstruktur [erstellen](#), [löschen](#), [umbenennen](#) und [verschieben](#).




Wichtig

Bitte beachten Sie Folgendes:

- Eine Gruppe kann sowohl Benutzer als auch andere Gruppen enthalten.
- Wenn Sie im linken Bereich eine Gruppe auswählen, können Sie alle Benutzer einsehen - außer denen, die in Untergruppen eingeordnet wurden. Wenn Sie alle Benutzer der Gruppe und ihrer Untergruppen anzeigen möchten, klicken Sie auf das Menü **Filter** am oberen Rand der Tabelle und wählen Sie **Alle Objekte rekursiv** im Bereich **Tiefe**.


Gruppen erstellen

So erstellen Sie eine benutzerdefinierte Gruppe:

1. Wählen Sie **Benutzerdefinierte Gruppen** im linken Fenster.
2. Klicken Sie auf die Schaltfläche  **Gruppe hinzufügen** im oberen Bereich des linken Fensters.
3. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK**. Die neue Gruppe wird jetzt unter **Benutzerdefinierte Gruppen** angezeigt.

Gruppen umbenennen

So benennen Sie eine benutzerdefinierte Gruppe um:

1. Wählen Sie im linken Fenster die Gruppe aus.
2. Klicken Sie auf die Schaltfläche  **Gruppe bearbeiten** im oberen Bereich des linken Fensters.
3. Geben Sie den neuen Namen in das entsprechende Feld ein.
4. Klicken Sie zur Bestätigung auf **OK**.

Gruppen und Benutzer verschieben

Innerhalb der Hierarchie **Benutzerdefinierte Gruppen** können Sie Gruppen und Benutzer beliebig verschieben. Um eine Gruppe oder einen Benutzer zu verschieben, verschieben Sie sie/ihn einfach per Drag und Drop von der derzeitigen Position zur neuen.



Beachten Sie

Die verschobene Entität erbt dabei die Richtlinieneinstellungen der neuen übergeordneten Gruppe, es sei denn, die Richtlinienvererbung wurde deaktiviert und eine andere Richtlinie zugewiesen.

Gruppen löschen

Eine Gruppe kann nicht gelöscht werden, wenn Sie mindestens einen Benutzer enthält. Wenn Sie eine Gruppe löschen möchten, verschieben Sie zunächst alle Benutzer in (eine) andere Gruppe(n). Wenn die Gruppe Untergruppen enthält, können Sie anstelle von einzelnen Benutzern auch alle Untergruppen verschieben.

Um eine Gruppe zu löschen:



1. Wählen Sie die leere Gruppe.
2. Klicken Sie auf die Schaltfläche  **Gruppe entfernen** im oberen Bereich des linken Fensters. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

6.4.4. Status der Mobilgeräte überprüfen

Jedes Mobilgerät wird auf der Netzwerkseite seinem Typ und Status entsprechend durch ein Symbol dargestellt.

Unter „[Netzwerkobjekttypen und -status](#)“ (S. 543) finden Sie eine Liste aller Symbole und Status.

Mobilgeräte können einen der folgenden Verwaltungsstatus haben:

-  **Verwaltet (Aktiv)** - wenn alle folgenden Bedingungen erfüllt sind:
 - GravityZone Mobile Client ist auf dem Gerät aktiviert.
 - GravityZone Mobile Client hat sich in den letzten 48 Stunden mit dem Control Center synchronisiert.
-  **Verwaltet (Leerlauf)** - wenn alle folgenden Bedingungen erfüllt sind:

- GravityZone Mobile Client ist auf dem Gerät aktiviert.
- GravityZone Mobile Client hat sich seit mindestens 48 Stunden nicht mehr mit dem Control Center synchronisiert.
- **Nicht verwaltet**, in den folgenden Situation:
 - GravityZone Mobile Client wurde noch nicht auf dem Mobilgerät installiert und aktiviert.
 - GravityZone Mobile Client wurde auf dem Mobilgerät deinstalliert (nur bei Android-Geräten).
 - Das Bitdefender-MDM-Profil wurde vom Gerät entfernt (nur bei iOS-Geräten).

So überprüfen Sie den Verwaltungsstatus von Geräten:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe, die Sie überprüfen möchten.
4. Klicken Sie auf das **Filtermenü** am oberen Rand der Tabelle und nehmen Sie die folgenden Einstellungen vor:
 - a. Gehen Sie zum Reiter **Ansicht** und wählen Sie **Geräte**.
 - b. Gehen Sie zum Reiter **Sicherheit** und wählen Sie im Bereich **Verwaltung** den Status, der Sie interessiert. Sie können ein oder mehrere Filterkriterien gleichzeitig auswählen.
 - c. Sie können auch alle Geräte rekursiv anzeigen, indem Sie die entsprechende Option im Reiter **Tiefe** markieren.
 - d. Klicken Sie auf **Speichern**.

Alle Mobilgeräte, die zu den entsprechenden Kriterien passen, werden in der Tabelle angezeigt.

Sie können auch einen Synchronisationsstatusbericht eines oder mehrerer Geräte generieren. Der Bericht enthält detaillierte Informationen zum Synchronisationsstatus jedes ausgewählten Geräts, darunter auch Datum und Uhrzeit der letzten Synchronisation. Weitere Informationen finden Sie unter [„Schnellberichte erstellen“ \(S. 195\)](#)

6.4.5. Konforme und Nicht-konforme Geräte

Nachdem die Anwendung GravityZone Mobile Client auf einem Mobilgerät aktiviert wurde, überprüft das Control Center, ob das Gerät alle Konformitätskriterien erfüllt. Mobilgeräte können einen der folgenden Sicherheitsstatus haben:

- **Ohne Sicherheitsprobleme** - wenn alle Konformitätskriterien erfüllt sind.
- **Mit Sicherheitsproblemen** - wenn mindestens ein Konformitätskriterium nicht erfüllt ist. Wenn ein Gerät für nicht-konform erklärt wird, wird der Benutzer aufgefordert, das Konformitätsproblem zu beheben. Der Benutzer muss dann innerhalb eines bestimmten Zeitrahmens die nötigen Änderungen vornehmen, da ansonsten die in der Richtlinie definierte Aktion für nicht-konforme Geräte angewendet wird.

Weitere Informationen zu Nichtkonformitätsaktionen und -kriterien finden Sie unter „[Konformität](#)“ (S. 416).

So überprüfen Sie den Konformitätsstatus von Geräten:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe, die Sie überprüfen möchten.
4. Klicken Sie auf das **Filtermenü** am oberen Rand der Tabelle und nehmen Sie die folgenden Einstellungen vor:
 - a. Gehen Sie zum Reiter **Ansicht** und wählen Sie **Geräte**.
 - b. Gehen Sie zum Reiter **Sicherheit** und wählen Sie im Bereich **Sicherheitsprobleme** den Status, der Sie interessiert. Sie können ein oder mehrere Filterkriterien gleichzeitig auswählen.
 - c. Sie können auch alle Geräte rekursiv anzeigen, indem Sie die entsprechende Option im Reiter **Tiefe** markieren.
 - d. Klicken Sie auf **Speichern**.
Alle Mobilgeräte, die zu den entsprechenden Kriterien passen, werden in der Tabelle angezeigt.
5. So können Sie das Verhältnis von konformen zu nicht konformen Geräten jedes Benutzers anzeigen:

- a. Klicken Sie auf das **Filtermenü** am oberen Rand der Tabelle und wählen Sie aus der Kategorie **Ansicht** den Punkt **Benutzer**. Alle Benutzer der ausgewählten Gruppe werden in der Tabelle angezeigt.
- b. In der Spalte **Konformität** sehen Sie, wie viele der Geräte dieses Benutzers konform sind.

Sie können auch einen Konformitätsbericht eines oder mehrerer Geräte generieren. Dieser Bericht enthält detaillierte Informationen zum Konformitätsstatus jedes ausgewählten Geräts, darunter auch etwaige Gründe für Nichtkonformität. Weitere Informationen finden Sie unter „[Schnellberichte erstellen](#)“ (S. 195)

6.4.6. Details zu Benutzern und Mobilgeräten anzeigen

Detaillierte Informationen zu jedem Benutzer und jedem Mobilgerät finden Sie auf der Seite **Netzwerk**.

Details zu Benutzern anzeigen

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe im linken Fenster.
4. Klicken Sie auf das **Filtermenü** am oberen Rand der Tabelle, wechseln Sie dann zum Reiter **Ansicht** und wählen Sie **Benutzer**. Um Benutzer rekursiv anzuzeigen, wechseln Sie zum Reiter **Tiefe** und wählen Sie dort **Alle Objekte rekursiv**. Klicken Sie auf **Speichern**. Alle Benutzer der ausgewählten Gruppe werden in der Tabelle angezeigt.
5. Die einzelnen Spalten enthalten verschiedene Informationen zu jedem Benutzer:
 - **Name**. Der Benutzername.
 - **Geräte**. Die Anzahl der Geräte dieses Benutzers. Klicken Sie auf die Zahl, um zur Ansicht **Geräte** zu gelangen und nur die entsprechenden Geräte anzuzeigen.
 - **Konformität**. Das Verhältnis von konformen zu nicht konformen Geräten dieses Benutzers. Klicken Sie auf den ersten Wert, um zur Ansicht **Geräte** zu wechseln und nur die konformen Geräte anzuzeigen.

6. Klicken Sie auf den Namen des Benutzers, der Sie interessiert. Ein Konfigurationsfenster wird angezeigt, in dem Sie den Namen und die E-Mail-Adresse des Benutzers anzeigen und bearbeiten können.

Details zu Geräten anzeigen

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe im linken Fenster.
4. Klicken Sie auf das **Filter**menü am oberen Rand der Tabelle, wechseln Sie dann zum Reiter **Ansicht** und wählen Sie **Geräte**. Klicken Sie auf **Speichern**. Alle Geräte aller Benutzer dieser Gruppe werden in der Tabelle angezeigt.
5. Die einzelnen Spalten der Tabelle enthalten verschiedene Informationen zu jedem Gerät:
 - **Name**. Der Name des Geräts.
 - **Benutzer**. Der Name des Benutzers, dem das entsprechende Gerät gehört.
 - **Betriebssystem**. Das Betriebssystem des Geräts.
6. Über einen Klick auf den Namen des Geräts erfahren Sie weitere Details. Das Fenster **Mobilgerätedetails** wird angezeigt, in dem Sie unter den Reitern **Überblick** und **Details** die folgenden Informationen einsehen können:
 - **Allgemein**.
 - **Name**. Der Name, der beim Hinzufügen des Geräts im Control Center angegeben wurde.
 - **Benutzer**. Der Name des Geräteeigentümers.
 - **Gruppe**. Die übergeordnete Gruppe des Geräts im Netzwerkinventar.
 - **Betriebssystem**. Das Betriebssystem des Geräts.
 - **Eigentümer**. Der Eigentümersertyp des Geräts (geschäftlich/enterprise oder privat).
 - **Sicherheit**.
 - **Client-Version**. Die Version der Anwendung GravityZone Mobile Client, die auf dem Gerät installiert ist; wird erst nach der Registrierung erkannt.

- **Richtlinie.** Die Richtlinie, die dem Mobilgerät zurzeit zugewiesen ist. Klicken Sie auf den Richtliniennamen, um zur entsprechenden Seite **Richtlinie** zu gelangen, auf der Sie die Sicherheitseinstellungen überprüfen können.



Wichtig

Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren. Änderungen an einer Richtlinie wirken sich auf sämtliche Geräte aus, denen diese Richtlinie zugewiesen wurde. Weitere Informationen finden Sie unter „[Richtlinien zuweisen](#)“ (S. 196).

- **Lizenzstatus.** Lizenzinformationen zum entsprechenden Gerät anzeigen.
- **Konformitätsstatus.** Der Konformitätsstatus ist für verwaltete Mobilgeräte verfügbar. Ein Mobilgerät kann konform oder nicht konform sein.



Beachten Sie

Für nicht konforme Mobilgeräte wird ein Symbol **!** angezeigt. Im Tooltip des Symbols steht der Grund für die Nicht-Konformität. Weitere Details zur Konformität von Mobilgeräten finden Sie unter „[Konformität](#)“ (S. 416).

- **Malware-Aktivität (Letzte 24 Stunden).** Ein schneller Überblick über die Menge gefundener Malware für das entsprechende Gerät an diesem Tag.
- **Sperrpasswort.** Ein einzigartiges Passwort, das bei der Registrierung des Geräts automatisch generiert wurde und zur **Fernsperrung** des Geräts verwendet wird (nur bei Android-Geräten).
- **Verschlüsselungsstatus.** Einige Geräte mit Android 3.0 oder neuer unterstützen die Geräteverschlüsselungsfunktion. Ob das entsprechende Gerät die Verschlüsselungsfunktion unterstützt, sehen Sie am Verschlüsselungsstatus auf der Geräte-Details-Seite. Wenn die Verschlüsselung per Richtlinie erforderlich ist, können Sie auch den Verschlüsselungssktivierungsstatus einsehen.
- **Aktivierungsdetails**
 - **Aktivierungs-Code.** Das dem Gerät zugewiesene einzigartige Aktivierungs-Token.

- Adresse des Kommunikations-Servers.
- **QR-Code.** Der einzigartige QR-Code, der die Adresse des Kommunikationsservers und das Aktivierungs-Token enthält.
- **Hardware.** Hier können Sie die Geräte-Hardware-Informationen einsehen; sie stehen nur für verwaltete (aktivierte) Geräte zur Verfügung. Hardware-Informationen werden alle 12 Stunden überprüft und gegebenenfalls aktualisiert.



Wichtig

Ab Android 10 hat GravityZone Mobile Client keinen Zugriff auf die Seriennummer, IMEI, IMSI und MAC-Adresse des Geräts. Diese Einschränkung hat die folgenden Auswirkungen:

- Wenn ein Mobilgerät, auf dem GravityZone Mobile Client bereits installiert ist, von einer älteren Android-Version auf Android 10 aktualisiert wird, zeigt das Control Center die korrekten Geräteinformationen an. Vor dem Upgrade muss auf dem Gerät bereits die neueste Version von GravityZone Mobile Client installiert sein.
 - Wird GravityZone Mobile Client auf einem Gerät mit Android 10 installiert, zeigt das Control Center aufgrund der durch das Betriebssystem bedingten Einschränkungen falsche Informationen zu diesem Gerät an.
- **Netzwerk.** Hier können Sie die Netzwerkverbindungs-Informationen einsehen; sie stehen nur für verwaltete (aktivierte) Geräte zur Verfügung.

6.4.7. Sortieren, Filtern und Suchen von Mobilgeräten

Je nach Anzahl der Benutzer und/oder Geräte kann die Inventartabelle für Mobilgeräte über mehrere Seiten gehen (standardmäßig werden pro Seite nur 10 Einträge angezeigt). Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Wenn die Tabelle sehr viele Einträge hat, können Sie die Filteroptionen nutzen, um nur diejenigen Entitäten anzuzeigen, die Sie interessieren. So können Sie zum Beispiel nach einem bestimmten Mobilgerät suchen oder nur verwaltete Mobilgeräte anzeigen.

Das Mobilgeräteinventar sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Wenn Sie zum Beispiel möchten, dass die Mobilgeräte nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**. Wenn Sie erneut auf die Überschrift klicken, werden die Mobilgeräte in umgekehrter Reihenfolge angezeigt.

Das Mobilgeräteinventar filtern

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Klicken Sie auf das **Filter**-Menü im oberen Bereich der Netzwerkfenster.
3. So verwenden Sie die Filterkriterien:
 - **Typ**. Wählen Sie die Art der Entitäten, die Sie anzeigen möchten (Benutzer/Geräte und Ordner).

Mobilgeräte - nach Art filtern

- **Sicherheit**. Zeigen Sie Computer nach Verwaltungs- und Sicherheitsstatus an.

Typ	Sicherheit	Richtlinie	Ansicht	Eigentümer	Tiefe
Verwaltung <input type="checkbox"/> Verwaltet (Aktiv) <input type="checkbox"/> Verwaltet (Leerlauf) <input type="checkbox"/> Nicht verwaltet		Sicherheitsprobleme <input type="checkbox"/> Mit Sicherheitsproblemen <input type="checkbox"/> Ohne Sicherheitsprobleme			
Ansicht: Geräte Tiefe: rekursiv					
Speichern		Abbrechen		Zurücksetzen	

Mobilgeräte - nach Sicherheit filtern

- Richtlinie.** Wählen Sie die Richtlinienvorlage, nach der Sie die Mobilgeräte filtern möchten, den Richtlinienzuweisungstyp (direkt oder geerbt) sowie den Richtlinienzuweisungsstatus (aktiv, angewendet oder ausstehend).

Typ	Sicherheit	Richtlinie	Ansicht	Eigentümer	Tiefe
Vorlage: <input type="text"/>					
Typ: <input type="checkbox"/> Direkt <input type="checkbox"/> Geerbt					
Status: <input type="checkbox"/> Aktiv <input type="checkbox"/> Angewendet <input type="checkbox"/> Ausstehend					
Ansicht: PCs Tiefe: in den ausgewählten Ordnern					
Speichern		Abbrechen		Zurücksetzen	

Mobilgeräte - nach Richtlinie filtern

- Anzeigen.** Wählen Sie **Benutzer**, um nur Benutzer der ausgewählten Gruppe anzuzeigen. Wählen Sie **Geräte**, um nur Geräte der ausgewählten Gruppe anzuzeigen.



Typ	Sicherheit	Richtlinie	Ansicht	Eigentümer	Tiefe
Ansicht					
<input type="radio"/> Benutzer <input checked="" type="radio"/> Geräte					
Ansicht: Geräte Tiefe: rekursiv					
Speichern		Abbrechen		Zurücksetzen	

Mobilgeräte - nach Ansicht filtern

- Eigentümer.** Sie können die Mobilgeräte nach Eigentümer filtern und entweder **Enterprise**-Geräte (Eigentum des Unternehmens) anzeigen oder **Privat**-Geräte. Das Attribut Eigentümer ist in den Mobilgerätedetails definiert.

Typ	Sicherheit	Richtlinie	Ansicht	Eigentümer	Tiefe
Anzeigen					
<input type="checkbox"/> Geschäftlich <input type="checkbox"/> Privat					
Ansicht: Geräte Tiefe: rekursiv					
Speichern		Abbrechen		Zurücksetzen	

Mobilgeräte - nach Eigentümer filtern

- Tiefe.** Bei der Verwaltung eines Netzwerks mit Baumstruktur werden Mobilgeräte oder Benutzer, die sich in Untergruppen befinden, bei Auswahl der Stammgruppe nicht angezeigt. Wählen Sie **Alle Objekte rekursiv**, um alle Entitäten der aktuellen Gruppe und ihrer Untergruppen anzuzeigen.

Typ	Sicherheit	Richtlinie	Ansicht	Eigentümer	Tiefe
Filtern nach					
<input type="radio"/> Objekte in den gewählten Ordnern					
<input checked="" type="radio"/> Alle Objekte rekursiv					
Ansicht: Geräte Tiefe: rekursiv					
Speichern		Abbrechen		Zurücksetzen	

Mobilgeräte - nach Tiefe filtern

4. Klicken Sie auf **Speichern**, um das Mobilgeräteinventar nach den gewählten Kriterien zu filtern.

Der Filter bleibt aktiv in der **Netzwerk**-Übersicht, bis Sie sich abmelden oder den Filter löschen.

Nach Mobilgeräten suchen

Die Tabelle im rechten Fenster enthält Einzelheiten zu Benutzern und Mobilgeräten. Über die Kategorien in jeder Spalte können Sie den Inhalt der Tabelle filtern.

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Wechseln Sie mithilfe des **Filtermenüs** am oberen Rand des Netzwerkfensterbereichs zur gewünschten Ansicht (Benutzer oder Mobilgeräte).
3. Suchen Sie mithilfe der Suchfelder unter jeder Spaltenüberschrift des rechten Fensters nach den gewünschten Entitäten:

- Geben Sie den gewünschten Suchbegriff in das entsprechende Suchfeld ein.

In der **Geräte**ansicht können Sie zum Beispiel den Namen eines Benutzers, den Sie suchen, in das Feld **Benutzer** eingeben. Nur die passenden Mobilgeräte werden in der Tabelle angezeigt.

- Wählen Sie das Attribut, nach dem Sie suchen möchten, aus dem entsprechenden Listenfeld.

Wechseln Sie zum Beispiel zur Ansicht **Geräte**, klicken Sie auf das Listenfeld **Betriebssystem** und wählen Sie **Android**, um nur Android-Mobilgeräte anzuzeigen.

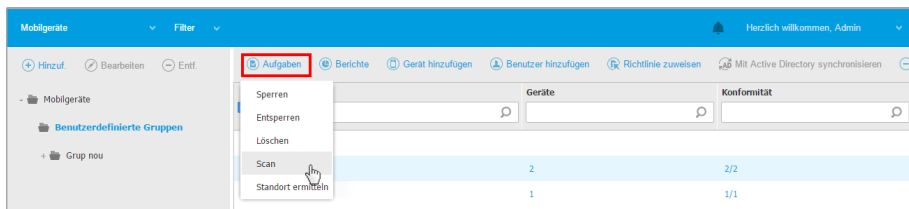
**Beachten Sie**

Um den Suchbegriff zu löschen und wieder alle Einträge anzuzeigen, bewegen Sie den Mauszeiger über das entsprechende Feld und klicken Sie auf das Symbol

6.4.8. Aufgaben auf Mobilgeräten ausführen

Über die Seite **Netzwerk** können Sie per Fernzugriff eine Reihe administrativer Aufgaben auf Mobilgeräten ausführen. Sie haben die folgenden Möglichkeiten:

- „Verriegeln“ (S. 191)
- „Löschen“ (S. 192)
- „Scan“ (S. 193)
- „Orten“ (S. 194)



Mobilgerätaufgaben

Damit Aufgaben per Fernzugriff auf Mobilgeräten ausgeführt werden können, müssen bestimmte Voraussetzungen erfüllt sein. Weitere Informationen finden Sie im Kapitel Installationsvoraussetzungen der GravityZone-Installationsanleitung.

Sie können Aufgaben individuell für einzelne Mobilgeräte, für einzelnen Benutzer oder für Gruppen von Benutzern erstellen. Sie können zum Beispiel per Fernzugriff die Mobilgeräte einer Gruppe von Benutzern auf Malware scannen. Sie können auch eine Ortungsaufgabe für ein bestimmtes Mobilgerät ausführen.

Das Netzwerkinventar kann Mobilgeräte enthalten, die **aktiv, im Leerlauf oder nicht verwaltet** sind. Sofort nach der Erstellung starten die Aufgaben auf aktiven Mobilgeräten. Auf Geräten im Leerlauf starten die Aufgaben erst, wenn die Geräte wieder online sind. Für nicht verwaltete Mobilgeräte werden Aufgaben nicht erstellt. In diesem Fall wird ein Hinweis angezeigt, dass die Aufgabe nicht erstellt werden konnte.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Verriegeln

Die Sperraufgabe sperrt sofort den Bildschirm des entsprechenden Mobilgeräts. Wie die Sperraufgabe genau ausgeführt wird, hängt vom Betriebssystem ab:

- Die Sperraufgaben für Android-Geräte (ab 7.0) erzwingen die Eingabe des über Ihre GravityZone-Konsole festgelegten Passworts nur dann, wenn auf dem Gerät kein Sperrschutz konfiguriert wurde. Andernfalls werden die bestehenden Optionen zum Sperren des Bildschirms wie Muster, PIN, Passwort, Fingerabdruck oder Smart Lock zum Schutz des Gerätes verwendet.




Beachten Sie

- Das vom Control Center generierte Passwort zur Entsperrung des Bildschirms wird im Fenster Mobilgerätedetails angezeigt.
 - Die Entsperraufgabe ist für Android-Geräte (ab 7.0) nicht mehr verfügbar. Stattdessen können Benutzer ihre Geräte manuell entsperren. Sie müssen jedoch im Voraus sicherstellen, dass diese Geräte die erwarteten Komplexitätsanforderungen für das Entsperrpasswort unterstützen.
 - Aus technischen Gründen steht die Sperraufgabe unter Android 11 nicht zur Verfügung.
- Auf iOS-Geräten mit einem bestehenden Passwort zur Entsperrung des Bildschirms wird dieses zum Entsperren abgefragt.

So führen Sie eine Fernsperrung eines Geräts durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
4. Klicken Sie auf das **Filter**menü am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Benutzer** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Benutzer der ausgewählten Gruppe werden in der Tabelle angezeigt.
5. Markieren Sie die Kästchen der Benutzer, die Sie interessieren. Sie können einen oder mehrere Benutzer gleichzeitig auswählen.

6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Sperren**.
7. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**. Eine Nachricht wird angezeigt, die besagt, ob die Aufgabe erstellt wurde oder nicht.
8. Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Löschen

Die Aufgabe **Löschen** setzt das entsprechende Gerät auf den Auslieferungszustand zurück. Diese Aufgabe können Sie ausführen, um alle vertraulichen Daten und Anwendungen auf dem Mobilgerät zu löschen.



Warnung

Setzen Sie die Aufgabe **Löschen** mit Bedacht ein. Überprüfen Sie, wem das Gerät gehört (wenn Sie keine privaten Geräte löschen möchten), und vergewissern Sie sich, dass Sie das entsprechende Gerät wirklich löschen möchten. Wenn die Aufgabe **Löschen** einmal gesendet wurde, kann sie nicht wieder rückgängig gemacht werden.



Beachten Sie

Aus technischen Gründen steht die Löschaufgabe unter Android 11 nicht zur Verfügung.


So führen Sie eine Fernlöschung eines Mobilgeräts durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
4. Klicken Sie auf das **Filtermenü** am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Geräte der ausgewählten Gruppe werden in der Tabelle angezeigt.



Beachten Sie

Wenn Sie alle Geräte der aktuellen Gruppe anzeigen möchten, können Sie im Bereich **Tiefe Alle Objekte rekursiv** wählen.

5. Markieren Sie das Kästchen für das Gerät, das Sie löschen möchten.
6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Löschen**.
7. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**. Eine Nachricht wird angezeigt, die besagt, ob die Aufgabe erstellt wurde oder nicht.
8. Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

Scan

Mit der Aufgabe **Scan** können Sie auf dem ausgewählten Gerät nach Malware suchen. Der Benutzer des Geräts wird über gefundene Malware informiert und aufgefordert, sie zu entfernen. Der Scan wird in der Cloud durchgeführt, weshalb der Dienst Zugang zum Internet benötigt.



Beachten Sie

Remote-Scans funktionieren auf iOS-Geräten nicht (aufgrund der Beschränkungen dieser Plattform).

So führen Sie einen Fern-Scan auf Mobilgeräten aus:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
4. Klicken Sie auf das **Filter**menü am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Geräte der ausgewählten Gruppe werden in der Tabelle angezeigt.





Beachten Sie

Wenn Sie alle Geräte der aktuellen Gruppe anzeigen möchten, können Sie im Bereich **Tiefe Alle Objekte rekursiv** wählen.

Um nur Android-Geräte in der ausgewählten Gruppe anzuzeigen, gehen Sie zur Spaltenüberschrift **Betriebssystem** im rechten Fenster, und wählen Sie **Android** aus dem entsprechenden Listenfeld.

5. Markieren Sie die Kästchen für die Geräte, die Sie scannen möchten.

6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Scan**.
7. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**. Eine Nachricht wird angezeigt, die besagt, ob die Aufgabe erstellt wurde oder nicht.
8. Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Wenn die Aufgabe ausgeführt wurde, steht eine Scan-Bericht zur Verfügung. Klicken Sie auf das entsprechende Symbol  in der Spalte **Berichte**, um einen Sofortbericht zu erstellen.

Weitere Informationen finden Sie unter „Aufgaben anzeigen und verwalten“ (S. 214).

Orten

Die Ortungsaufgabe öffnet eine Karte, auf der der Standort des Geräts eingezeichnet ist. Sie können ein oder mehrere Geräte gleichzeitig orten.

Damit die Aufgabe Ortung funktioniert, müssen die Ortungsdienste auf dem Mobilgerät aktiviert sein.


So orten Sie ein Mobilgerät:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
4. Klicken Sie auf das **Filter**menü am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Geräte der ausgewählten Gruppe werden in der Tabelle angezeigt.



Beachten Sie


Wenn Sie alle Geräte der aktuellen Gruppe rekursiv anzeigen möchten, können Sie im Bereich **Tiefe Alle Objekte rekursiv** wählen.

5. Markieren Sie das Kästchen für das Gerät, das Sie orten möchten.
6. Klicken Sie auf die Schaltfläche  **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Standort ermitteln**.
7. Das Fenster **Standort** wird angezeigt, das folgende Informationen enthält:

- Eine Karte, auf der der Standort des ausgewählten Mobilgeräts eingezeichnet ist. Wenn ein Gerät nicht synchronisiert ist, zeigt die Karte den letzte bekannten Standort des Geräts an.
 - Eine Tabelle mit den Details zu den ausgewählten Geräten (Name, Benutzer, Datum und Uhrzeit letzte Synchronisation). Sie können den Standort eines bestimmten Geräts, das in der Tabelle aufgeführt ist, auf der Karte anzeigen, indem Sie sein Kästchen markieren. Die Karte wird automatisch auf den Standort des entsprechenden Geräts zentriert.
 - Mit der Option **Automatisch neu laden** wird der Standort des ausgewählten Geräts automatisch alle 10 Sekunden neu ermittelt.
8. Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter „[Aufgaben anzeigen und verwalten](#)“ (S. 214).

6.4.9. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte zu verwalteten Mobilgeräten erstellen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.
4. Klicken Sie auf das **Filter**menü am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Sie können auch im Reiter **Sicherheit** die Veraltet-Option wählen, um die ausgewählte Gruppe nach verwalteten Geräten zu filtern. Klicken Sie auf **Speichern**. Alle Geräte der ausgewählten Gruppe, die den Filterkriterien entsprechen, werden in der Tabelle angezeigt.
5. Markieren Sie die Kästchen der gewünschten Mobilgeräte. Sie können einen oder mehrere Geräte gleichzeitig auswählen.
6. Klicken Sie auf die Schaltfläche  **Bericht** am oberen Rand der Tabelle, und wählen Sie den Berichtstyp aus dem Menü. Weitere Informationen finden Sie unter „[Berichte zu Mobilgeräten](#)“ (S. 457)
7. Konfigurieren Sie die Berichtsoptionen. Weitere Informationen finden Sie unter „[Berichte erstellen](#)“ (S. 459)

8. Klicken Sie auf **Generieren**. Der Bericht wird sofort angezeigt. Es dauert unterschiedlich lange, bis Berichte erstellt sind, je nach Anzahl der ausgewählten Mobilgeräte.

6.4.10. Richtlinien zuweisen

Über **Richtlinien** können Sie Sicherheitseinstellungen auf Mobilgeräte verwalten. Im Bereich **Netzwerk** können Sie Richtlinien für Mobilgeräte in Ihrem Konto anzeigen, ändern und zuweisen.

Richtlinien können Sie Gruppen, Benutzern oder bestimmten Mobilgeräten zuweisen.

Beachten Sie

Eine Richtlinie, die einem Benutzer zugewiesen ist, gilt für alle Geräte dieses Benutzers. Weitere Informationen finden Sie unter „[Zuweisung von lokalen Richtlinien](#)“ (S. 231).


So zeigen Sie die Sicherheitseinstellungen eines Mobilgeräts an:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Klicken Sie auf das **Filtermenü** am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Geräte aller Benutzer dieser Gruppe werden in der Tabelle angezeigt.
4. Klicken Sie auf den Namen des Geräts, für das Sie sich interessieren. Das Fenster [Details](#) wird angezeigt.
5. Klicken Sie auf der Seite **Produktübersicht** im Bereich **Sicherheit** auf den Namen der aktuell zugewiesenen Richtlinie, um ihre Einstellungen anzuzeigen.
6. Sie können die Sicherheitseinstellungen nach Bedarf ändern. Bitte beachten Sie, dass Ihre Änderungen sich auch auf alle anderen Geräte auswirken, auf denen die Richtlinie aktiv ist.

Weitere Informationen finden Sie unter „[Richtlinien für Mobilgeräte](#)“ (S. 410)

So weisen Sie einem Mobilgerät eine Richtlinie zu:


1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe, die Sie überprüfen möchten.

4. Klicken Sie auf das **Filter**menü am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**. Klicken Sie auf **Speichern**. Alle Geräte aller Benutzer dieser Gruppe werden in der Tabelle angezeigt.
5. Markieren Sie im rechten Fenster das Kästchen des Mobilgeräts, das Sie interessiert.
6. Klicken Sie auf die Schaltfläche  **Richtlinie zuweisen** am oberen Ende der Tabelle.
7. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor. Weitere Informationen finden Sie unter „[Zuweisung von lokalen Richtlinien](#)“ (S. 231).

6.4.11. Synchronisation mit Active Directory

Das Netzwerkinventar wird automatisch nach einem im Konfigurationsbereich des Control Center festgelegten Intervall mit Active Directory synchronisiert. Weitere Informationen finden Sie im Kapitel "GravityZone Installation und Einrichtung" der GravityZone-Installationsanleitung.

So synchronisieren Sie die aktuell angezeigten Benutzer mit Active Directory:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Klicken Sie auf die Schaltfläche  **Mit Active Directory synchronisieren** am oberen Rand der Tabelle.
4. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.



Beachten Sie

Bei großen Active-Directory-Netzwerken kann die Synchronisation eine Weile dauern.

6.4.12. Benutzer und Mobilgeräte löschen

Wenn sich obsoleter Benutzer oder Geräte im Netzwerkinventar befinden, empfehlen wir, sie zu löschen.

Mobilgeräte aus dem Netzwerkinventar löschen

Nach der Löschung eines Geräts aus dem Control Center gilt Folgendes:

- Die Verknüpfung von GravityZone Mobile Client wird aufgehoben, es wird aber nicht vom Gerät entfernt.
- Auf iOS-Geräten wird das MDM-Profil entfernt. Wenn das Gerät nicht mit dem Internet verbunden ist, bleibt das MDM-Profil installiert, bis eine neue Verbindung verfügbar ist.
- Sämtliche Protokolle, die sich auf das gelöschte Gerät beziehen, sind weiterhin verfügbar.
- Ihre persönlichen Daten und Anwendungen werden nicht tangiert.



Warnung

- Gelöschte Mobilgeräte können Sie nicht wiederherstellen.
- Wenn Sie versehentlich ein gesperrtes Gerät löschen, müssen Sie es auf den Auslieferungszustand zurücksetzen, um es zu entsperren.

So löschen sie Mobilgeräte:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe, die Sie überprüfen möchten.
4. Klicken Sie auf das **Filtermenü** am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Geräte** aus der Kategorie **Ansicht**.
5. Klicken Sie auf **Speichern**.
6. Markieren Sie die Kästchen der Mobilgeräte, die Sie löschen möchten.
7. Klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Benutzer aus dem Netzwerkinventar löschen

Derzeit mit Mobilgeräten verknüpfte Benutzer können nicht gelöscht werden. Sie müssen zuerst das entsprechende Mobilgeräte löschen.



Beachten Sie

Sie können nur Benutzer aus Benutzerdefinierten Gruppen löschen.

So löschen Sie einen Benutzer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie **Mobilgeräte** aus der [Ansichtsauswahl](#).
3. Wählen Sie im linken Fenster die Gruppe, die Sie überprüfen möchten.
4. Klicken Sie auf das **Filtermenü** am oberen Rand des Netzwerkfensterbereichs und wählen Sie **Benutzer** aus der Kategorie **Ansicht**.
5. Klicken Sie auf **Speichern**.
6. Markieren Sie das Kästchen des Benutzers, den Sie löschen möchten.
7. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

6.5. Anwendungsbestand

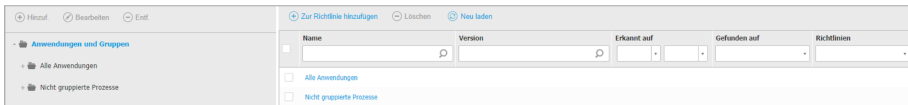
Sie können alle in Ihrem Netzwerk ermittelten Anwendungen über die Aufgabe **Anwendungserkennung** im Bereich **Anwendungen und Gruppen** anzeigen. Weitere Informationen finden Sie unter „[Anwendungserkennung](#)“ (S. 103).

Die Anwendungen und Prozesse werden automatisch zum Ordner **Anwendungen und Gruppen** im Fenster links hinzugefügt.

Sie können Anwendungen und Prozesse in benutzerdefinierten Gruppen zusammenfassen.

Alle Anwendungen/Prozesse in einem ausgewählten Ordner werden in der Tabelle im rechten Fenster angezeigt. Sie können nach Name, Version, Veröffentlichter/Autor, Updater, Standort und Richtlinien suchen.

Klicken Sie oben in der Tabelle auf **Neu laden**, um die neuesten Informationen in der Tabelle anzuzeigen. Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.



Anwendungsbestand



Wichtig

Neue Anwendungen, die über die Aufgabe **Anwendungserkennung** ermittelt werden, werden automatisch im Ordner **Nicht gruppierte Anwendungen** abgelegt. Prozesse,

die nicht zu einer bestimmten Anwendung gehören, werden im Ordner **Nicht gruppierte Prozesse** abgelegt.

Baumansicht Anwendungen und Gruppen

So können Sie der Baumansicht **Anwendungen und Gruppen** eine benutzerdefinierte Gruppe hinzufügen:

1. Wählen Sie den Ordner **Alle Anwendungen** aus.
2. Klicken Sie oben in der Baumansicht auf die Schaltfläche **+Hinzufügen**.
3. Ein neues Fenster wird geöffnet. Geben Sie hier einen Namen ein.
4. Klicken Sie auf **OK**, um die neue Gruppe anzulegen.
5. Wählen Sie den Ordner **Nicht gruppierte Anwendungen** aus. Alle Anwendungen, die in einem ausgewählten Ordner zusammengefasst wurden, werden in der Tabelle im rechten Fenster angezeigt.
6. Wählen Sie die gewünschten Anwendungen aus der Tabelle im Fenster rechts aus. Ziehen Sie die ausgewählten Objekte per Drag und Drop vom Fenster rechts in die gewünschte benutzerdefinierte Gruppe im Fenster links.

So können Sie eine benutzerdefinierte Anwendung hinzufügen:


1. Wählen Sie unter **Alle Anwendungen** den Zielordner aus.
2. Klicken Sie oben in der Baumansicht auf die Schaltfläche **+Hinzufügen**.
3. Ein neues Fenster wird geöffnet. Geben Sie hier einen Namen ein.
4. Klicken Sie auf **OK**, um die benutzerdefinierte Anwendung anzulegen.
5. Sie können Prozesse, die zu der neuen benutzerdefinierten Anwendung gehören, über den Ordner **Nicht gruppierte Prozesse** oder über andere Ordner in der Baumansicht **Anwendungen und Gruppen** hinzufügen. Nach der Auswahl des Ordners werden alle Prozesse in der Tabelle im Fenster rechts angezeigt.
6. Wählen Sie die gewünschten Prozesse aus der Tabelle im Fenster rechts aus. Ziehen Sie die ausgewählten Objekte per Drag & Drop vom Fenster links in die benutzerdefinierte Anwendung.



Beachten Sie

Eine Anwendung kann nur zu jeweils einer Gruppe gehören.

So können Sie einen Ordner oder Anwendungsnamen bearbeiten:


1. Wählen Sie ihn aus der Baumansicht **Anwendungen und Gruppen** aus.
2. Klicken Sie oben in der Baumansicht auf die Schaltfläche  **Bearbeiten**.
3. Geben Sie einen neuen Namen ein.
4. Klicken Sie auf **OK**.

Innerhalb der Hierarchie **Anwendungen und Gruppen** können Sie Gruppen und Anwendungen beliebig verschieben. Um eine Gruppe oder Anwendung zu verschieben, ziehen Sie sie einfach per Drag & Drop von der derzeitigen Position zur neuen.

Um benutzerdefinierte Ordner oder Anwendungen zu entfernen, wählen Sie sie in der Baumansicht **Anwendungen und Gruppen** aus und klicken Sie auf die  **Entfernen**-Schaltfläche oben in der Baumansicht.

Anwendungen zu Richtlinien hinzufügen

So können Sie eine Anwendung oder einen Prozess direkt über den Anwendungsbestand hinzufügen:

1. Wählen Sie den gewünschten Ordner aus der Baumansicht **Anwendungen und Gruppen** aus. Die Inhalte des Ordners werden im Fenster rechts angezeigt.
2. Wählen Sie die gewünschten Prozesse oder Anwendungen aus dem Fenster rechts aus.
3. Klicken Sie auf die Schaltfläche  **Zur Richtlinie hinzufügen**, um das Konfigurationsfenster zu öffnen.
4. Geben Sie im Bereich **Regel auf diese Richtlinien anwenden** einen bestehenden Richtliniennamen ein. Über das Suchfeld können Sie nach Richtliniennamen oder Eigentümer suchen.
5. Geben Sie im Bereich **Regeldetails** einen **Regelnamen** ein.
6. Markieren Sie das Kästchen **Aktiviert**, um die Regel zu aktivieren.
7. Der Zieltyp wird automatisch erkannt. Bei Bedarf können Sie bereits bestehende Kriterien bearbeiten:
 - **Bestimmter Prozess oder Prozesse** zur Definition eines Prozesses, dessen Ausführung zugelassen oder verweigert werden soll. Die Autorisierung kann nach Pfad, Hash oder Zertifikat erfolgen. Die Regelbedingungen können über ein logisches UND verknüpft werden.

- So können Sie eine Anwendung über einen bestimmten Pfad autorisieren:
 - a. Wählen Sie in der Spalte **Typ** den Eintrag **Pfad** aus. Geben Sie den Pfad zum Objekt an. Sie können einen absoluten oder relativen Pfadnamen eingeben oder Platzhalter verwenden. Das Sternchen (*) steht für jede Datei innerhalb eines Verzeichnisses. Zwei Sternchen (**) stehen für alle Dateien und Verzeichnisse im definierten Verzeichnis. Ein Fragezeichen (?) steht für genau ein beliebiges Zeichen. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.
 - b. Wählen Sie aus dem Klappmenü **Wählen Sie einen oder mehrere Kontexte aus**. lokal, CR-ROM, Wechselmedium oder Netzwerk aus. Sie können Anwendungen, die über Wechselmedien ausgeführt werden, blockieren oder ihre Ausführung nur lokal erlauben.
- Um Anwendungen anhand ihres Hashs zu autorisieren, wählen Sie in der Spalte **Typ** den Eintrag **Hash** aus und geben Sie einen Hash-Wert ein. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.

**Wichtig**

Zu Erzeugung des Hash-Werts können Sie das [Fingerprint-Tool](#) herunterladen. Weitere Informationen finden Sie unter „[Tools der Anwendungssteuerung](#)“ (S. 548)

- Zur Autorisierung anhand eines Zertifikats wählen Sie in der Spalte **Typ** den Eintrag **Zertifikat** aus und geben Sie einen Zertifikatfingerabdruck ein. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.

**Wichtig**

Zum Erhalt des Zertifikatfingerabdrucks können Sie das [Thumbprint-Tool](#) herunterladen. Weitere Informationen finden Sie unter „[Tools der Anwendungssteuerung](#)“ (S. 548)

Allgemein

Name der Regel:

Aktiviert

Ziele

Ziel:

Zertifikat	Geben Sie einen Zertifikatfingerabdruck ein.	Geben Sie einen Wert ein.	Wählen Sie einen oder mehrere Kontexte.	
Typ	Übereinstimmung	Beschreibung	Kontext	Aktion
Pfad	C:\test*.exe	**wildcard	Lokal	⊗
Pfad	C:\test\test1*.exe	*wildcard	Lokal	⊗
Pfad	C:\test\test1\exemp?e.exe	? wildcard	Lokal	⊗
Hash	aabbccddeeffgghh6789	hash beschreibung	N/A	⊗
Zertifikat	aaddggyy1234567890	zertifikat beschreibung	N/A	⊗

Anwendungsregeln

Klicken Sie auf **+** **Hinzufügen** die Regel hinzuzufügen. Der neu angelegten Regel wird in dieser Richtlinie höchste Priorität eingeräumt.

- **Bestandsanwendungen oder -gruppen** zum Hinzufügen von im Ihrem Netzwerk ermittelten Gruppen oder Anwendungen. Sie können die in Ihrem Netzwerk ausgeführten Anwendungen auf der Seite **Netzwerk- > Anwendungsbestand** einsehen.


Geben Sie die Namen der Anwendungen oder Gruppen durch Komma getrennt in das Feld ein. Die Funktion zum automatischen Einfügen zeigt schon während der Eingabe Vorschläge an.

8. Markieren Sie das Kästchen **Auch untergeordnete Prozesse**, um die Regel auch auf Kindprozesse anzuwenden.

⊗ **Warnung**


Wir empfehlen, diese Option bei der Festlegung von Regeln für Browser-Anwendungen zu deaktivieren, um Sicherheitsrisiken zu vermeiden.

9. Sie können optional auch Ausschlüsse von der Prozessstartregel festlegen. Das Hinzufügen ähnelt der bereits im beschriebenen Vorgehensweise.


10. Im Bereich **Berechtigungen** legen Sie fest, ob die Regelausführung zugelassen oder verweigert werden soll.
11. Klicken Sie **Speichern**, um die Änderungen zu speichern.
So können Sie eine Anwendung oder einen Prozess löschen:
 1. Wählen Sie den gewünschten Ordner aus der Baumansicht **Anwendungen und Gruppen** aus.
 2. Wählen Sie die gewünschten Prozesse oder Anwendungen aus dem Fenster rechts aus.
 3. Klicken Sie auf die Schaltfläche  **Löschen**.

Updater

Sie müssen für die in Ihrem Netzwerk ermittelten Anwendungen Updater festlegen.

-  **Warnung**
Wenn Sie keine Updater zuweisen, werden Updates für die Anwendungen auf der Whitelist nicht zugelassen.


So können Sie einen Updater zuweisen:

1. Wählen Sie den gewünschten Ordner in der Baumansicht **Anwendungen und Gruppen** aus. Die Inhalte des Ordners werden im Fenster rechts angezeigt.
2. Wählen Sie im Fenster rechts die Datei aus, die Sie als Updater verwenden möchten.
3. Klicken Sie auf die Schaltfläche  **Updater zuweisen**.
4. Klicken Sie **Ja**, um die Zuweisung zu bestätigen. Updater werden mit einem eigenen Symbol markiert:



Updater

So können Sie einen Updater verwerfen:

1. Wählen Sie den gewünschten Ordner in der Baumansicht **Anwendungen und Gruppen** aus. Die Inhalte des Ordners werden im Fenster rechts angezeigt.
2. Wählen Sie im Fenster rechts den Updater aus, den Sie verwerfen möchten.
3. Klicken Sie auf die Schaltfläche  **Updater verwerfen**.
4. Klicken Sie zur Bestätigung auf **Ja**.

6.6. Patch-Inventar

GravityZone findet alle von Ihrer Software benötigten Patches durch **Patch-Scan**-Aufgaben und fügt sie dann dem Patch-Inventar hinzu.

Auf der Seite **Patch-Inventar** werden alle Patches angezeigt, die für die auf Ihren Endpunkten installierte Software gefunden wurden. Für die Patches stehen Ihnen verschiedene Aktionen zur Auswahl.

Verwenden Sie das Patch-Inventar, um bestimmte Patches sofort zu installieren. So können Sie einfach und schnell bestimmte Probleme beheben, die Ihnen bereits bekannt sind. So zum Beispiel wenn Sie einen Artikel über eine Softwareschwachstelle gelesen haben und die CVE-ID bereits kennen. Sie können das Inventar nach Patches speziell für diese CVE durchsuchen und danach die Endpunkte anzeigen, die aktualisiert werden sollten.

Sie können das Patch-Inventar über das Hauptmenü des Control Centers mit einem Klick auf **Netzwerk > Patch-Inventar** aufrufen.

Die Seite ist in zwei Bereiche unterteilt:

- Auf der linken Seite finden Sie die in Ihrem Netzwerk installierte Software nach Anbieter geordnet.
- Auf der rechten Seite finden Sie eine Tabelle mit einer Übersicht der verfügbaren Patches und weiteren Informationen.

Dashboard		Search products...		Ignore patches		Install		Patch stats		Refresh			
Network		Display all patches											
Patch Inventory													
Application Inventory													
Packages													
Tasks													
Policies													
Assignment Rules													
Patch Name	KB Nu...	CVE	Bullet...	Patch sever...	Category	Installed / Pendi...	Missing / Install...	Affected Pr...					
<input type="checkbox"/>	Windows6.1-SP1-Windows7-KB...	Q24799...	1 CVE(s)	MS11-0...	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)				
<input type="checkbox"/>	Windows6.1-SP1-Windows7-KB...	Q25054...	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)				
<input type="checkbox"/>	Windows6.1-SP1-Windows7-KB...	Q24881...	0 CVE(s)	MSWU...	None	Non-Security	0 EP / 0 EP	1 EP / 0 EP	6 Product(s)				
<input type="checkbox"/>	Windows6.1-Windows7-SP1-KB...	Q24916...	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)				
<input type="checkbox"/>	Windows6.1-Windows7-SP1-KB...	Q25062...	1 CVE(s)	MS11-0...	Important	Security	0 EP / 0 EP	1 EP / 0 EP	7 Product(s)				

Patch-Inventar

Im nächsten Schritt erfahren Sie, wie Sie das Inventar nutzen können. Sie haben die folgenden Möglichkeiten:

- [Anzeigen von Patch-Details](#)
- [Suchen und Filtern von Patches](#)
- [Patches ignorieren](#)
- [Installieren von Patches](#)
- [Deinstallieren von Patches](#)
- [Erstellen von Patch-Statistiken](#)

6.6.1. Anzeigen von Patch-Informationen


In der Tabelle mit den Patches finden Sie Informationen, die Ihnen dabei helfen, bestimmte Patches zu finden, Ihre Dringlichkeit einzuschätzen sowie den Installationsstatus und -umfang zu bestimmen. Die verfügbaren Informationen werden im Folgenden näher beschrieben:

- **Patch-Name.** Der Name der ausführbaren Datei, die den Patch enthält.
- **KB-Nummer.** Diese Nummer weist auf den Artikel in der Wissensdatenbank hin, der den Patch-Release ankündigt.
- **CVE.** Die Nummer der CVE, die durch den Patch behoben wird. Mit einem Klick auf diese Nummer wird die Liste der CVE-IDs angezeigt.
- **Bulletin-ID.** Die ID des vom Anbieter veröffentlichten Security Bulletins. Diese ID verlinkt den eigentlichen Artikel, der den Patch beschreibt und Informationen zur Installation bereitstellt.
- **Schweregrad des Patches.** Anhand dieser Bewertung können Sie die Dringlichkeit des Patches im Verhältnis zu den vermiedenen Schäden einschätzen.
- **Kategorie.** Patches werden anhand der von ihnen behobenen Probleme in zwei Kategorien unterteilt: sicherheitsrelevant und nicht sicherheitsrelevant. Dieses Feld informiert Sie über die Patch-Kategorie.
- **Installiert / Installation ausstehend.** Diese Zahlen zeigen an, auf wie vielen Endpunkten das Patch bereits installiert wurde und auf wie vielen Endpunkten die Patch-Installation noch aussteht. Die Zahlen verlinken jeweils auf eine Liste mit diesen Endpunkten.

- **Fehlt / Installation fehlgeschlagen.** Diese Zahlen zeigen an, auf wie vielen Endpunkten das Patch noch nicht installiert wurde und auf wie vielen Endpunkten die Installation fehlgeschlagen ist. Die Zahlen verlinken jeweils auf eine Liste mit diesen Endpunkten.
- **Betroffene Produkte.** Die Anzahl der Produkte, für die das Patch veröffentlicht wurde. Die Zahl verlinkt auf eine Liste mit diesen Softwareprodukten.
- **Entfernbar.** Falls Sie ein bestimmtes Patch wieder zurücksetzen möchten, müssen Sie zunächst prüfen, ob es deinstalliert werden kann. Verwenden Sie diesen Filter, um herauszufinden, welche Patches entfernbare sind (zurückgesetzt werden können). Weitere Informationen finden Sie unter [Deinstallieren von Patches](#).

Gehen Sie folgendermaßen vor, um die in der Tabelle angezeigten Details anzupassen:

1. Klicken Sie auf die Schaltfläche **III Spalten** auf der rechten Seite der [Symbolleiste](#).
2. Wählen Sie die Spalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um zur Standardansicht zurückzukehren.

Während die Seite aufgerufen ist, können im Hintergrund laufende GravityZone-Prozesse die Datenbank beeinflussen. Klicken Sie oben in der Tabelle auf  **Neu laden**, um sicherzustellen, dass die neuesten Informationen in der Tabelle angezeigt werden.

GravityZone überprüft einmal wöchentlich die Liste der verfügbaren Patches und löscht diejenigen, die nicht mehr anwendbar sind, weil entweder die zugehörigen Anwendungen oder die Endpunkte nicht mehr vorhanden sind.

GravityZone überprüft und löscht auch täglich die Patches, die in der Liste nicht verfügbar sind, obwohl sie auf einigen Endpunkten vorhanden sein können.

6.6.2. Suchen und Filtern von Patches

Das Control Center zeigt standardmäßig alle für Ihre Software verfügbaren Patches an. GravityZone bietet eine Reihe von Optionen zum schnellen Auffinden der benötigten Patches.

Filtern von Patches nach Produkt

1. Suchen Sie das Produkt im Bereich links.

Scrollen Sie dazu durch die Liste um den entsprechenden Anbieter zu finden oder geben Sie den Namen in das Suchfeld oben ein.



2. Klicken Sie auf den Namen des Anbieters, um die Liste zu erweitern und die Produkte anzuzeigen.
3. Wählen Sie Produkt aus, um die verfügbaren Patches anzuzeigen, oder heben Sie die Auswahl auf, um die Patches zu verbergen.
4. Wiederholen Sie die vorausgegangenen Schritte für alle anderen Produkte, für die Sie sich interessieren.

Wenn Sie wieder die Patches für alle Produkte anzeigen möchten, klicken Sie oben rechts im Bereich links auf **Alle Patches anzeigen**.

Filtern von Patches nach Nützlichkeit

Ein Patch wird nicht mehr benötigt, wenn dieses Patch oder eine neuere Version bereits auf dem Endpunkt bereitgestellt wurde. Da das Inventar unter Umständen auch solche Patches auch weiterhin anzeigt, erlaubt es GravityZone diese zu ignorieren. Wählen Sie die entsprechenden Patches aus und klicken Sie danach am oberen Rand der Tabelle auf **Patches ignorieren**.

Das Control Center zeigt die ignorierten Patches dann in einer anderen Ansicht an. Klicken Sie auf der rechten Seite der [Symbolleiste](#) auf **Verwaltet/Ignoriert**, wenn Sie die Ansicht wechseln möchten:

-  um ignorierte Patches anzuzeigen.
-  um verwaltete Patches anzuzeigen.

Filtern von Patches nach Details

Nutzen Sie die Suchfunktionen, um Patches nach bestimmten Kriterien oder bekannten Details zu filtern. Geben Sie die Suchbegriffe in die Suchfelder am oberen Rand der Patch-Tabelle ein. Die entsprechenden Patches werden dann in der Tabelle schon bei der Eingabe bzw. nach erfolgter Auswahl angezeigt.


Durch das Löschen der Suchbegriffe wird die Suche zurückgesetzt.

6.6.3. Ignorieren von Patches




Wenn Sie bestimmte Patches nicht auf Ihren Endpunkten installieren möchten, können Sie diese mit dem Befehl **Patches ignorieren** aus dem Scan-Inventar ausschließen.

Ignorierte Patches werden automatisch von den Patch-Aufgaben und Patch-Berichten ausgeschlossen und gelten nicht als fehlende Patches.

So können Sie Patches ignorieren:

1. Wählen Sie auf der Seite **Patch-Inventar** den oder die Patches aus, die Sie ignorieren möchten.
2. Klicken Sie am oberen Rand der Tabelle auf  **Patches ignorieren**.
In dem Konfigurationsfenster, das jetzt angezeigt wird, können Sie Details zu den ausgewählten Patches sowie alle untergeordneten Patches einsehen.
3. Klicken Sie auf **Ignorieren**. Dieser Patch wird aus der Patch-Inventar-Liste entfernt.

Sie können die ignorierten Patches in einer eigenen Ansicht aufrufen und entsprechende Aktionen ausführen:

- Klicken Sie oben rechts in der Tabelle auf  **Ignorierte Patches anzeigen**. Eine Liste mit allen ignorierten Patches wird angezeigt.
- Durch Erstellen eines Patch-Statistik-Berichts können Sie weitere Informationen über ein bestimmtes ignoriertes Patch abrufen. Wählen Sie das gewünschte ignorierte Patch aus und klicken Sie am oberen Rand der Tabelle auf  **Patch-Statistiken**. Weitere Einzelheiten finden Sie unter „Patch-Statistiken erstellen“ (S. 213)
- Klicken Sie zur Wiederherstellung von ignorierten Patches am oberen Rand der Tabelle auf  **Patches wiederherstellen**.
In dem Konfigurationsfenster, das jetzt angezeigt wird, können Sie Details zu den ausgewählten Patches einsehen.
Klicken Sie auf **Wiederherstellen**, um die Patches in das Inventar zu verschieben.


6.6.4. Installieren von Patches

Gehen Sie folgendermaßen vor, um Patches über das Patch-Inventar zu installieren:

1. Öffnen Sie **Netzwerk > Patch-Inventar**.
2. Suchen Sie die Patches, die Sie installieren möchten. Verwenden Sie dazu bei Bedarf zum schnellen Auffinden die Filteroptionen.
3. Wählen Sie die entsprechenden Patches aus und klicken Sie danach am oberen Rand der Tabelle auf  **Installieren**. In dem Konfigurationsfenster, das jetzt angezeigt wird, können Sie die Details zur Patch-Installation bearbeiten.

Die ausgewählten Patches werden gemeinsam mit den untergeordneten Patches angezeigt.

- Wählen Sie die Zielendpunktgruppen aus.
- **Falls nötig, Endpunkte nach Installation des Patches neu starten.** Durch Auswahl dieser Option werden die Endpunkte unmittelbar nach der Patch-Installation neu gestartet, wenn ein Systemstart erforderlich ist. Bitte bedenken Sie, dass diese Aktion Benutzer bei der Arbeit stören könnte.

Bleibt diese Option deaktiviert, wird auf den Zielendpunkten, auf denen ein Neustart erforderlich ist, das  Symbol für den ausstehenden Neustart im GravityZone-Netzwerkinventar angezeigt. Dabei haben Sie die folgenden Möglichkeiten:

- Eine **Computer neu starten**-Aufgabe zu einem beliebigen Zeitpunkt an alle Endpunkte übermitteln, auf denen ein Neustart aussteht. Weitere Informationen finden Sie unter [„Computer neu starten“ \(S. 101\)](#).
- Die aktive Richtlinien so konfigurieren, dass der Endpunktbenutzer über die Notwendigkeit eines Neustarts benachrichtigt wird. Rufen Sie dazu die aktive Richtlinie für den Zielendpunkt auf, gehen Sie zu **Allgemein> Benachrichtigungen** und aktivieren Sie die Option **Benachrichtigung über Endpunktneustart**. Der Benutzer wird ab sofort mit einem Pop-up-Fenster benachrichtigt, wenn ein Neustart aufgrund von Änderungen durch die angegebenen GravityZone-Komponenten (in diesem Fall Patch-Verwaltung) erforderlich ist. Das Pop-up bietet die Option, den Neustart zu verschieben. Wenn der Benutzer sich entscheidet, den Neustart zu verschieben, wird die Neustartbenachrichtigung in regelmäßigen Abständen so lange angezeigt, bis das System neu gestartet wurde oder die vom Unternehmensadministrator festgelegte Zeit abgelaufen ist.

Weitere Informationen finden Sie unter [„Benachrichtigung über Endpunktneustart“ \(S. 251\)](#).

4. Klicken Sie auf **Installieren**.

Die Installationsaufgabe wird gemeinsam mit allen Unteraufgaben für jeden Zielendpunkt erstellt.

i Beachten Sie

- Ausgehend von den Endpunkten, die Sie verwalten möchten, können Sie ein Patch auch über die **Netzwerk**-Seite installieren. Wählen Sie dazu die Endpunkte aus dem Netzwerkinventar aus, klicken Sie am oberen Rand der Tabelle auf die **Aufgaben**-Schaltfläche und klicken Sie danach auf **Patch-Installation**. Weitere Informationen finden Sie im Kapitel „Patch-Installation“ (S. 85).
- Nach Installation eines Patches empfiehlt es sich, eine **Patch-Scan**-Aufgabe an die Zielpunkte zu übermitteln. Durch diese Aktion werden die in GravityZone gespeicherten Patch-Informationen für Ihre verwalteten Netzwerke aktualisiert.

6.6.5. Deinstallieren von Patches

Es kann vorkommen, dass Sie Patches, die Fehlfunktionen auf den Zielpunkten verursacht haben, wieder entfernen müssen. GravityZone umfasst eine Funktion zum Zurücksetzen von in Ihrem Netzwerk installierten Patches. So können Sie die Software wieder auf den Stand vor Anwendung des Patches zurückversetzen.

Diese Funktion zur Deinstallation ist nur für entfernbare Patches verfügbar. Im GravityZone-Patch-Inventar finden Sie die Spalte **Entfernbar**, um Patches nach Entfernbarkeit zu filtern.

i Beachten Sie


Ob ein Patch entfernbare ist oder nicht, hängt davon ab, wie das Patch vom Hersteller herausgegeben wurde bzw. welche Änderungen das Patch an der Software vorgenommen hat. Bei nicht entfernbaren Patches kann es notwendig werden, die Software erneut zu installieren.


So können Sie ein Patch deinstallieren:

1. Öffnen Sie **Netzwerk > Patch-Inventar**.
2. Wählen Sie das Patch aus, das Sie deinstallieren möchten. Über die Filtern in den Spalten, so z. B. KB-Nummer oder CVE, können Sie nach bestimmten Patches suchen. Verwenden Sie die Spalte **Entfernbar**, um nur die verfügbaren Patches anzuzeigen, die deinstalliert werden können.

i Beachten Sie

Sie können jeweils nur ein Patch für einen oder mehrere Endpunkte deinstallieren.

3. Klicken Sie am oberen Rand der Tabelle auf die Schaltfläche  **Deinstallieren**. In dem Konfigurationsfenster, das jetzt angezeigt wird, können Sie die Details zur Patch-Deinstallation bearbeiten.

- **Aufgabenname.** Sie können den Standardnamen für die Patch-Deinstallationsaufgabe bei Bedarf ändern. Auf diese Weise können Sie die Aufgabe in der **Aufgaben**-Übersicht leichter finden.
- **Patch zur Liste der ignorierten Patches hinzufügen.** In der Regel wird ein Patch, das deinstalliert werden soll, nicht mehr benötigt. Mit dieser Option wird das Patch automatisch nach Abschluss der Patch-Deinstallation zur **Liste der ignorierten Patches** hinzugefügt.
- **Falls nötig, Endpunkte nach Deinstallation des Patches neu starten.** Durch Auswahl dieser Option werden die Endpunkte unmittelbar nach der Patch-Deinstallation neu gestartet, wenn ein Systemstart erforderlich ist. Bitte bedenken Sie, dass diese Aktion Benutzer bei der Arbeit stören könnte. Bleibt diese Option deaktiviert, wird auf den Zielendpunkten, auf denen ein Neustart erforderlich ist, das  Symbol für den ausstehenden Neustart im GravityZone-Netzwerkinventar angezeigt. Dabei haben Sie die folgenden Möglichkeiten:

- Eine **Computer neu starten**-Aufgabe zu einem beliebigen Zeitpunkt an alle Endpunkte übermitteln, auf denen ein Neustart aussteht. Weitere Informationen finden Sie unter „**Computer neu starten**“ (S. 101).
- Die aktive Richtlinien so konfigurieren, dass der Endpunktbenutzer über die Notwendigkeit eines Neustarts benachrichtigt wird. Rufen Sie dazu die aktive Richtlinie für den Zielendpunkt auf, gehen Sie zu **Allgemein > Benachrichtigungen** und aktivieren Sie die Option **Benachrichtigung über Endpunktneustart**. Der Benutzer wird ab sofort mit einem Pop-up-Fenster benachrichtigt, wenn ein Neustart aufgrund von Änderungen durch die angegebenen GravityZone-Komponenten (in diesem Fall Patch-Verwaltung) erforderlich ist. Das Pop-up bietet die Option, den Neustart zu verschieben. Wenn der Benutzer sich entscheidet, den Neustart zu verschieben, wird die Neustartbenachrichtigung in regelmäßigen Abständen angezeigt, bis der Benutzer das System neu startet oder bis die im Feld Unternehmensadministrator festgelegte Zeit abgelaufen ist.

Weitere Informationen finden Sie unter „**Benachrichtigung über Endpunktneustart**“ (S. 251).

- Wählen Sie in der Tabelle **Ziele zurücksetzen** die Endpunkte aus, von denen Sie das Patch deinstallieren möchten.

Sie können einen oder mehrere Endpunkte in Ihrem Netzwerk auswählen. Nutzen Sie die verfügbaren Filter, um den gewünschten Endpunkt zu finden.



Beachten Sie

Die Tabelle zeigt nur die Endpunkte, auf denen das ausgewählte Patch installiert ist.

4. Klicken Sie auf **Bestätigen**. Eine Aufgabe zur **Patch-Deinstallation** wird erstellt und an den Zielendpunkt übermittelt.

Für jede abgeschlossene Patch-Deinstallationsaufgabe wird automatisch ein Bericht zur **Patch-Deinstallation** erstellt. Hier finden Sie Details zu dem Patch, den Zielendpunkten und dem Status der Patch-Deinstallationsaufgabe.




Beachten Sie

Nach Deinstallation eines Patches empfiehlt es sich, eine **Patch-Scan**-Aufgabe an die Zielendpunkte zu übermitteln. Durch diese Aktion werden die in GravityZone gespeicherten Patch-Informationen für Ihre verwalteten Netzwerke aktualisiert.

6.6.6. Patch-Statistiken erstellen

Wenn Sie Details zum Status eines bestimmten Patches für alle Endpunkte benötigen, können Sie über die Funktion **Patch-Statistiken** einen Sofortbericht für den ausgewählten Patch erstellen:

1. Wählen Sie auf der Seite **Patch-Inventar** auf der rechten Seite den gewünschten Patch.
2. Klicken Sie auf die Schaltfläche  **Patch-Statistiken** am oberen Rand der Tabelle. Ein Patch-Statistikbericht wird angezeigt, der verschiedene Details zum Patch-Status anzeigt, darunter:
 - Ein Tortendiagramm mit den Prozentsätzen Endpunkte, auf denen der Patch als installiert, fehlgeschlagen, fehlend und ausstehend gemeldet wurde.
 - Eine Tabelle mit den folgenden Informationen:
 - **Name, FQDN, IP-Adresse** und **Betriebssystem** für jeden Endpunkt, der den Patch gemeldet hat.

- **Letzte Prüfung:** der Zeitpunkt, zu dem der Patch zuletzt auf dem Endpunkt geprüft wurde.
- **Patch-Status:** installiert, fehlgeschlagen, fehlend oder ignoriert.



Beachten Sie

Die Patch-Statistik-Funktion steht für verwaltete und ignorierte Patches zur Verfügung.

6.7. Aufgaben anzeigen und verwalten

Auf der Seite **Netzwerk > Aufgaben** können Sie alle Aufgaben, die Sie erstellt haben, einsehen und verwalten.

Sobald Sie eine Aufgabe für Netzwerkobjekte erstellt haben, wird sie in der Aufgabentabelle aufgeführt.

Auf der Seite **Netzwerk > Aufgaben** haben Sie folgende Möglichkeiten:

- [Aufgabenstatus überprüfen](#)
- [Aufgabenberichte anzeigen](#)
- [Aufgaben neu starten](#)
- [Exchange-Scan-Aufgaben anhalten](#)
- [Aufgaben löschen](#)

6.7.1. Aufgabenstatus überprüfen

Wenn Sie eine Aufgabe für Netzwerkobjekte erstellen, werden Sie den Fortschritt der Aufgabe überprüfen wollen und benachrichtigt werden, wenn Fehler auftreten.

Auf der Seite **Netzwerk > Aufgaben** informiert Sie die Spalte **Status** der einzelnen Aufgaben über den jeweiligen Status. Sie können den Status der Hauptaufgabe überprüfen und detaillierte Informationen über jede Teilaufgabe abrufen.

<input type="button" value="Neustart"/> <input type="button" value="Löschen"/> <input type="button" value="Neu laden"/>					
Name	Aufgabentyp	Status	Startintervall	Berichte	
<input type="checkbox"/> Quick Scan 2015-10-09	Scan	Ausstehend (0 / 1)	09 Okt 2015, 10:51:44		

Die Aufgabenübersicht

- **Status der Hauptaufgabe überprüfen.**

Die Hauptaufgabe ist die Aktion, die auf die Netzwerkobjekte angewendet wird (wie zum Beispiel Installation des Clients oder Scan). Sie enthält bestimmte Teilaufgaben, eine für jedes Netzwerkobjekt. So enthält eine Installationshauptaufgabe für acht Computer zum Beispiel acht Teilaufgaben. Die Zahlen in Klammern geben an, wie viele Teilaufgaben schon abgeschlossen wurden. So bedeutet (2/8) zum Beispiel, dass zwei von acht Teilaufgaben abgeschlossen sind.

Die Hauptaufgabe kann einen der folgenden Status haben:

- **Ausstehend** - wenn noch keine der Teilaufgaben gestartet wurde oder wenn die Anzahl der gleichzeitigen Installation überschritten ist. Die maximale Anzahl der gleichzeitigen Installationen kann im Menü **Konfiguration** festgelegt werden. Weitere Informationen hierzu finden Sie in der GravityZone-Installationsanleitung.
- **Wird ausgeführt** - wenn alle Teilaufgaben laufen. Die Hauptaufgabe bleibt in diesem Status, bis die letzte Teilaufgabe abgeschlossen ist.
- **Fertig**, wenn alle Teilaufgaben (erfolgreich oder erfolglos) beendet wurden. Bei erfolglosen Teilaufgaben wird ein Warnsymbol angezeigt.

- **Status der Teilaufgaben überprüfen.**

Gehen Sie zur Aufgabe, die Sie interessiert, und klicken Sie auf den Link in der Spalte **Status**, um das Fenster **Status** zu öffnen. Dort werden die Netzwerkobjekte, auf die die Hauptaufgabe sich bezieht, sowie der Status jeder Teilaufgabe angezeigt. Die Teilaufgaben können folgende Status haben:

- **Wird ausgeführt** - wenn die Teilaufgabe noch läuft.
Für Exchange-Bedarf-Scan-Aufgaben können Sie zusätzlich den Abschlussstatus anzeigen.
- **Fertig** - wenn die Teilaufgabe erfolgreich abgeschlossen wurde.
- **Ausstehend** - wenn die Teilaufgabe noch nicht gestartet wurde. Das kann in den folgenden Situationen passieren:
 - Die Teilaufgabe wartet in einer Warteschlange.
 - Es gibt Verbindungsprobleme zwischen der Control Center und dem Zielobjekt im Netzwerk.
 - Das Zielgerät ist im Leerlauf (offline) - im Falle von Mobilgeräten. Die Aufgabe wird auf dem Zielgerät ausgeführt, sobald es wieder online ist.

- **Fehlgeschlagen** - wenn die Teilaufgabe nicht gestartet werden konnte oder wegen eines Fehlers wie ungültigen Zugangsdaten oder zu geringem Speicher angehalten wurde.
- **Angehalten**, wird angezeigt, wenn der Bedarf-Scan zu lange gedauert hat und Sie ihn angehalten haben.

Sie können Details zu einzelnen Teilaufgaben anzeigen, indem Sie sie auswählen und im Bereich **Details** unten in der Tabelle nachsehen.

The screenshot shows a 'Task Status' window with a search bar and a 'Refresh' button. Below is a table with columns 'Computer Name' and 'Status'. One row is visible for 'SRV2012' with a status of 'Pending'. Below the table is a pagination control showing 'Page 1 of 1' and '1 items'. A 'Details' section below the table shows 'Created on: 21 Oct 2015, 14:55:06' and a 'Close' button.

Aufgabenstatusdetails


Dort finden Sie die folgenden Informationen:

- Datum und Uhrzeit des Aufgabenstarts.
- Datum und Uhrzeit des Aufgabenendes.
- Beschreibung aufgetretener Fehler.

6.7.2. Aufgabenberichte anzeigen


Auf der Seite **Netzwerk > Aufgaben** können Sie Schnellberichte zu Scan-Aufgaben lesen.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Wählen Sie das gewünschte Netzwerkobjekt aus der [Ansichtsauswahl](#).
3. Markieren Sie das Kästchen der Scan-Aufgabe, die Sie interessiert.

4. Klicken Sie auf die entsprechende Schaltfläche  in der Spalte **Berichte**. Warten Sie, bis der Bericht angezeigt wird. Weitere Informationen finden Sie unter „[Berichte verwenden](#)“ (S. 438).

6.7.3. Aufgaben werden neu gestartet

Die Client-Installation, Deinstallation oder Update-Aufgaben können aus verschiedenen Gründen fehlschlagen. Sie müssen solche fehlgeschlagenen Aufgaben nicht neu anlegen, sondern können sie wie folgt neu starten:

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Wählen Sie das gewünschte Netzwerkobjekt aus der [Ansichtsauswahl](#).
3. Markieren Sie die Kästchen für die fehlgeschlagenen Aufgaben.
4. Klicken Sie auf die Schaltfläche  **Starten** am oberen Rand der Tabelle. Die ausgewählten Aufgaben werden neu gestartet und der Aufgabenstatus wechselt auf **Neuer Versuch**.




Beachten Sie

Bei Aufgaben mit mehreren Teilaufgaben ist die Option **Starten** nur dann verfügbar, wenn alle Teilaufgaben abgeschlossen wurden. Es werden nur die fehlgeschlagenen Teilaufgaben erneut ausgeführt.

6.7.4. Anhalten von Exchange-Scan-Aufgaben

Ein Scan des Exchange-Informationsspeichers kann erhebliche Zeit in Anspruch nehmen. Wenn Sie eine Bedarf-Scan-Aufgabe für Exchange aus irgendeinem Grund anhalten möchten, gehen Sie folgendermaßen vor:


1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Wählen Sie die gewünschte Netzwerkansicht aus der [Ansichtsauswahl](#) aus.
3. Klicken Sie auf den Link in der **Status**-Spalte, um das **Aufgabenstatus**-Fenster zu öffnen.
4. Aktivieren Sie die Kästchen für die ausstehende oder laufende Unteraufgabe, die Sie anhalten möchten.
5. Klicken Sie auf die Schaltfläche  **Aufgaben anhalten** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

**Beachten Sie**

Sie können einen Bedarf-Scan des Exchange-Informationsspeichers auch über den Ereignisbereich in Bitdefender Endpoint Security Tools anhalten.

6.7.5. Aufgaben löschen

GravityZone löscht ausstehende Aufgaben automatisch nach 2 Tagen, abgeschlossene Aufgaben nach 30 Tagen. Sollten Sie immer noch viele Aufgaben haben, empfehlen wir, nicht mehr benötigte Aufgaben zu löschen, um die Liste übersichtlich zu halten.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Wählen Sie das gewünschte Netzwerkobjekt aus der [Ansichtsauswahl](#).
3. Markieren Sie das Kästchen der Aufgabe, die Sie löschen möchten.
4. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

**Warnung**

Wenn Sie eine ausstehende Aufgabe löschen, wird die Aufgabe auch abgebrochen. Wenn eine laufende Aufgabe gelöscht wird, werden etwaige ausstehende Teilaufgaben abgebrochen. In diesem Fall können abgeschlossene Teilaufgaben nicht rückgängig gemacht werden.

6.8. Endpunkte aus dem Netzwerkinventar löschen

Das Netzwerkinventar enthält standardmäßig den Ordner **Gelöscht**, in dem Endpunkte gespeichert sind, die Sie nicht verwalten möchten.

Die **Löschen**-Aktion hat folgende Auswirkungen:

- Wenn nicht verwaltete Endpunkte gelöscht werden, werden Sie direkt in den Ordner **Gelöscht** verschoben.
- Bei Löschung von verwalteten Endpunkten:
 - Eine Client-deinstallieren-Aufgabe wird angelegt
 - Ein Lizenzplatz wird freigegeben
 - Die Endpunkte werden in den Ordner **Gelöscht** verschoben.

So löschen Sie Endpunkte aus dem Netzwerkinventar:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die passende Netzwerkansicht aus der **Ansichtsauswahl**.
3. Wählen Sie **Benutzerdefinierte Gruppen** im linken Fenster. Alle Endpunkte dieser Gruppe werden in der Tabelle im rechten Fenster angezeigt.

**Beachten Sie**

Sie können nur Endpunkte unter **Benutzerdefinierte Gruppen** löschen, die außerhalb von integrierten Netzwerkinfrastrukturen gefunden wurden.

4. Markieren Sie im rechten Fenster das Kästchen des Endpunktes, den Sie löschen möchten.
5. Klicken Sie auf die Schaltfläche **☒ Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Wird ein verwalteter Endpunkt gelöscht, wird eine **Client deinstallieren**-Aufgabe auf der Seite **Aufgaben** erstellt und der Sicherheitsagent wird von dem Endpunkt deinstalliert. Dadurch wird ein Lizenzplatz frei.

6. Der Endpunkt wird in den Ordner **Gelöscht** verschoben.

Sie können Endpunkte aus dem Ordner **Gelöscht** jederzeit mit der Maus nach **Benutzerdefinierte Gruppen** ziehen.

**Beachten Sie**

- Wenn Sie bestimmte Endpunkte dauerhaft von der Verwaltung ausschließen möchten, müssen diese in dem Ordner **Gelöscht** verbleiben.
- Wenn Sie Endpunkte aus dem Ordner **Gelöscht** löschen, werden diese vollständig aus der GravityZone-Datenbank entfernt. Ausgeschlossene Endpunkte die online sind, werden dennoch auch weiterhin bei Ausführung einer Netzwerkerkennungsaufgabe gefunden und im Netzwerkinventar als neue Endpunkte angezeigt.

6.9. Konfigurieren von Netzwerkeinstellungen

Auf der Seite **Konfiguration > Netzwerkeinstellungen** können Sie Einstellungen für das Netzwerkinventar konfigurieren, so z. B.: Speichern von Filtern, Beibehalten des zuletzt durchsuchten Speicherorts, Erstellen und Verwalten von geplanten Regeln zum Löschen nicht verwendeter virtueller Maschinen.

Die Optionen sind in die folgenden Bereiche unterteilt:

- [Netzwerkinventareinstellungen](#)
- [Offline-Maschinen-Bereinigung](#)

6.9.1. Netzwerkinventareinstellungen

Im Abschnitt **Netzwerkinventareinstellungen** finden Sie die folgenden Optionen:

- **Filter für Netzwerkinventar speichern.** Markieren Sie dieses Kästchen, um Ihre Filter auf der Seite **Netzwerk** von einer Control Center-Sitzung zur nächsten zu speichern.
- **Letzte aufgerufene Position im Netzwerkinventar bis zu meiner Abmeldung merken.** Markieren Sie dieses Kästchen, um die letzte aufgerufene Position zu speichern, wenn Sie die Seite **Netzwerk** verlassen. Die Position wird zwischen den Sitzungen nicht gespeichert.
- **Vermeiden Sie Duplikate von geklonten Endpunkten.** Mit dieser Option schalten Sie eine neue Art von Netzwerkobjekten in GravityZone frei: Golden Images. Hiermit können Sie die ursprünglichen Endpunkte von deren Klonen unterscheiden. Dazu müssen Sie jeden Endpunkt, den Sie in Zukunft klonen möchten, wie folgt markieren:
 1. Gehen Sie zur Seite **Netzwerk**.
 2. Wählen Sie den Endpunkt, den Sie klonen möchten.
 3. Wählen Sie im Kontextmenü den Punkt **Als Golden Image markieren**.

6.9.2. Offline-Maschinen-Bereinigung

Im Abschnitt **Offline-Maschinen-Bereinigung** können Sie Regeln für das automatische Löschen ungenutzter virtueller Maschinen aus dem Netzwerkinventar anlegen.

Tasks	Offline machines cleanup																								
Risk Management	Configure rules to automatically delete unused virtual machines from the Network Inventory and clear their license seats.																								
Policies	+ Add rule X Delete																								
Assignment Rules																									
Reports	<table border="1"> <thead> <tr> <th>Rule name</th> <th>Offline for</th> <th>Machines name</th> <th>Location</th> <th>Deleted(last 24h)</th> <th>State</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> <input type="text" value=""/></td> <td><input type="text" value=""/></td> <td><input type="text" value=""/></td> <td><input type="text" value=""/></td> <td><input type="text" value=""/></td> <td><input type="text" value=""/></td> </tr> <tr> <td><input type="checkbox"/> Rule 3</td> <td>66 days</td> <td>...</td> <td>Custom Groups</td> <td>0 machines</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/> Rule 4</td> <td>78 days</td> <td>...</td> <td>Custom Groups</td> <td>0 machines</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Rule name	Offline for	Machines name	Location	Deleted(last 24h)	State	<input type="checkbox"/> <input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="checkbox"/> Rule 3	66 days	...	Custom Groups	0 machines	<input checked="" type="checkbox"/>	<input type="checkbox"/> Rule 4	78 days	...	Custom Groups	0 machines	<input type="checkbox"/>
Rule name	Offline for	Machines name	Location	Deleted(last 24h)	State																				
<input type="checkbox"/> <input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>																				
<input type="checkbox"/> Rule 3	66 days	...	Custom Groups	0 machines	<input checked="" type="checkbox"/>																				
<input type="checkbox"/> Rule 4	78 days	...	Custom Groups	0 machines	<input type="checkbox"/>																				
Quarantine																									
Accounts																									
User Activity																									
System Status																									
Configuration																									
Update																									

Konfiguration - Netzwerkeinstellungen - Offline-Maschinen-Bereinigung

Regeln erstellen

So können Sie eine Bereinigungsregel erstellen:

1. Klicken Sie im Abschnitt **Offline-Maschinen-Bereinigung** auf die Schaltfläche **Regel hinzufügen**.
2. Wechseln Sie zur Konfigurationsseite:
 - a. Geben Sie einen Namen für die Regel ein.
 - b. Legen Sie eine Uhrzeit für die tägliche Bereinigung fest.
 - c. Legen Sie die Bereinigungskriterien fest:
 - Die Anzahl der Tage, an denen die Maschinen offline waren (von 1 bis 90).
 - Ein Namensmuster, das auf eine oder auf mehrere virtuelle Maschinen zutreffen kann.
Verwenden Sie beispielsweise `machine_1`, um die Maschine mit diesem Namen zu löschen. Alternativ können Sie mit `machine_*` alle Maschinen löschen, deren Name mit `machine_` beginnt.
In diesem Feld ist Groß- und Kleinschreibung relevant. Außerdem dürfen nur Buchstaben, Ziffern und die Sonderzeichen Asterisk (*), Unterstrich (_), Bindestrich (-) verwendet werden. Der Name darf nicht mit einem Asterisk (*) beginnen.
 - d. Wählen Sie die Gruppe von Endpunkten im Netzwerkinventar, auf die die Regel angewendet werden soll.
3. Klicken Sie auf **Speichern**.

Anzeigen und Verwalten von Regeln

Im Abschnitt **Netzwerkeinstellungen > Offline-Maschinen-Bereinigung** werden alle von Ihnen erstellten Regeln angezeigt. In einer eigenen Tabelle finden Sie die folgenden Details:

- Name der Regel.
- Die Anzahl der Tage, seit die Maschinen offline gegangen sind.
- Namensmuster der Maschinen.
- Ort im Netzwerkinventar.
- Die Anzahl der in den letzten 24 Stunden gelöschten Maschinen.
- Zustand: aktiviert, deaktiviert oder ungültig.



Beachten Sie

Eine Regel ist ungültig, wenn die Ziele aus irgendeinem Grund nicht mehr gültig sind. Wenn z. B. die virtuellen Maschinen gelöscht wurden oder Sie keinen Zugriff mehr auf sie haben.

Neu erstellte Regeln werden standardmäßig aktiviert. Sie können Regeln jederzeit über den Ein-/Aus-Schalter in der Spalte **Zustand** aktivieren und deaktivieren.

Nutzen Sie bei Bedarf die Sortierungs- und Filtermöglichkeiten am oberen Rand der Tabelle, um nach bestimmten Regeln zu suchen.

So können Sie eine Regel ändern:

1. Klicken Sie auf den Namen der Regel.
2. Bearbeiten Sie auf der Konfigurationsseite die Details der Regel.
3. Klicken Sie auf **Speichern**.

So können Sie eine oder mehrere Regeln löschen:

1. Verwenden Sie die Kästchen, um eine oder mehrere Regeln auszuwählen.
2. Klicken Sie am oberen Rand der Tabelle auf **Löschen**.

6.10. Konfigurieren von Security Server-Einstellungen

Security Server verwenden ihren Caching-Mechanismus zur Deduplizierung der Malware-Scans und optimieren so diesen Prozess. Der nächste Schritt zur

Scan-Optimierung ist die gemeinsame Nutzung dieses Caches durch verschiedene Security Server.

Cache-Sharing ist nur zwischen Security Servern des gleichen Typs möglich. So teilt ein Security Server Multi-Platform seinen Cache z. B. nur mit einem anderen Security Server Multi-Platform und nicht mit einem Security Server für NSX.

So aktivieren und konfigurieren Sie die gemeinsame Cache-Nutzung:

1. Rufen Sie die Seite **Konfiguration > Security Server-Einstellungen** auf.
2. Markieren Sie das Kästchen **Gemeinsame Cache-Nutzung durch Security Server**
3. Legen Sie den Umfang der gemeinsamen Nutzung fest:

- Alle verfügbaren Security Server.

Diese Option wird empfohlen, wenn sich alle Security Server im selben Netzwerk befinden.

- In der Zuweisungsliste verfügbare Security Server.

Verwenden Sie diese Option, wenn die Security Server auf verschiedene Netzwerken verteilt sind und die gemeinsame Nutzung des Caches ein hohes Datenaufkommen erzeugen könnte.

4. Erstellen Sie zur Einschränkung des Umfangs eine Gruppe von Security Servern. Wählen Sie die Security Server aus der Dropdownliste aus und klicken Sie auf **Hinzufügen**.

Nur die Security Server in der Tabelle stellen ihren Cache für die gemeinsame Nutzung bereit.



Beachten Sie

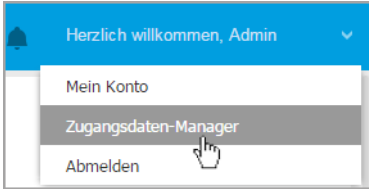
Security Server für NSX-T und NSX-V tauschen Cache-Informationen nur innerhalb desselben vCenter Servers aus.

5. Klicken Sie auf **Speichern**.

6.11. Zugangsdaten-Manager

Der Zugangsdaten-Manager hilft Ihnen dabei, die Zugangsdaten festzulegen, die zum Zugriff auf die verfügbaren vCenter-Server-Inventare sowie zur Fernauthentifizierung bei verschiedenen Betriebssystemen in Ihrem Netzwerk benötigt werden.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.



Das Zugangsdaten-Manager-Menü

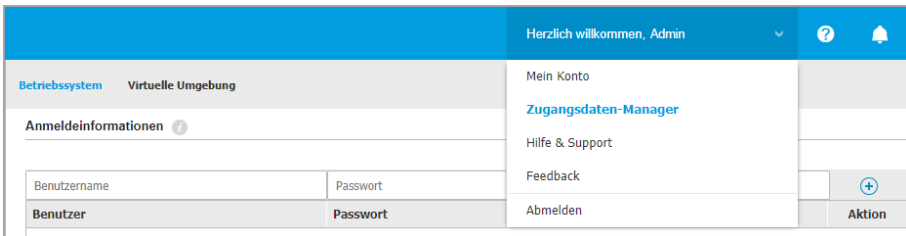
Das Fenster **Zugangsdaten-Manager** hat zwei Reiter:

- [Betriebssystem](#)
- [Virtuelle Umgebung](#)

6.11.1. Betriebssystem

Im Reiter **Betriebssystem** können Sie die Administrator-Zugangsdaten verwalten, die für die Fernauthentifizierung während der Ausführung von Installationsaufgaben auf Computern und virtuellen Maschinen in Ihrem Netzwerk nötig sind.

So fügen Sie Zugangsdaten hinzu:



Zugangsdaten-Manager

1. Geben Sie in die entsprechenden Felder im oberen Bereich der Tabelle den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

Bei der Eingabe des Namens eines Nutzerkontos Windows-Konvention verwenden:

- Für Active Directory-Maschinen wird folgende Syntax verwendet: `username@domain.com` und `Domäne\Benutzername`. Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).
 - Bei Arbeitsgruppen-Maschinen genügt die Eingabe des Benutzernamens ohne Angabe des Namens der Arbeitsgruppe.
2. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.



Beachten Sie

Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

6.11.2. Virtuelle Umgebung

Im Reiter Virtuelle Umgebung können Sie die Zugangsdaten für die verfügbaren virtuellen Server-Systeme verwalten.

Um auf die mit dem Control Center integrierte virtuelle Infrastruktur zugreifen zu können, müssen Sie Ihre Benutzerzugangsdaten für jedes verfügbare virtualisierte Server-System angeben. Control Center stellt mithilfe Ihrer Zugangsdaten eine Verbindung zur virtualisierten Infrastruktur her und zeigt nur diejenigen Ressourcen an, auf die Sie Zugriff haben (wie im virtualisierten Server definiert).

So legen Sie die Zugangsdaten fest, die für die Verbindung zu einem virtualisierten Server nötig sind:

1. Wählen Sie den Server aus dem entsprechenden Menü.



Beachten Sie

Wenn das Menü nicht verfügbar ist, wurde entweder noch keine Integration konfiguriert oder alle nötigen Zugangsdaten wurden bereits konfiguriert.

2. Geben Sie Ihren Benutzernamen und Ihr Passwort und eine aussagekräftige Beschreibung ein.
3. Klicken Sie auf den Button **Hinzufügen**. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.

**Beachten Sie**

Wenn Sie Ihre Zugangsdaten zur Authentifizierung nicht im Zugangsdaten-Manager konfigurieren, müssen Sie sie angeben, sobald Sie das Inventar irgendeines Virtualisierte-Server-Systems durchsuchen. Wenn Sie Ihre Zugangsdaten einmal eingegeben haben, werden sie im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

**Wichtig**

Wenn Sie Ihr Passwort für Ihren virtualisierten Server ändern, müssen Sie es auch im Zugangsdaten-Manager aktualisieren.

6.11.3. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsoletere Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile. Das ausgewählte Konto wird gelöscht.

7. SICHERHEITSRICHTLINIEN

Nach der Installation kann der Bitdefender-Schutz über das Control Center mit Hilfe von Sicherheitsrichtlinien konfiguriert und verwaltet werden. Eine Richtlinie legt die Sicherheitseinstellungen fest, die auf bestimmten Netzwerkinventarobjekten (Computern, virtuellen Maschinen oder Mobilgeräten) angewendet werden sollen.

Direkt nach der Installation wird den Netzwerkinventarobjekten die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist. Wurde die NSX-Integration aktiviert, stehen drei weitere Standardsicherheitsrichtlinien für NSX zur Verfügung, eine für jedes Sicherheitsniveau: tolerant, normal und aggressiv. Diese Richtlinien sind mit den empfohlenen Sicherheitseinstellungen vorkonfiguriert. Die Standardrichtlinien können Sie weder ändern noch löschen.

Sie können ganz nach Ihren Sicherheitsanforderungen für jede Art von verwaltetem Netzwerkobjekt beliebig viele Richtlinien erstellen.

Was Sie über Richtlinien wissen sollten:

- Richtlinien werden in der **Richtlinienübersicht** erstellt und in der **Netzwerkübersicht** den Netzwerkobjekten zugewiesen.
- Richtlinien können mehrere Moduleinstellungen von anderen Richtlinien erben.
- Richtlinienzuweisung an Endpunkten lässt sich so konfigurieren, dass eine Richtlinie nur unter bestimmten Bedingungen gilt, je nach Standort oder eingeloggtem Benutzer. Aus diesem Grund kann ein Endpunkt mehrere zugewiesene Richtlinien haben.
- Endpunkte können nur jeweils eine aktive Richtlinie haben.
- Sie können eine Richtlinie einzelnen Endpunkten oder Gruppen von Endpunkten zuweisen. Wenn Sie eine Richtlinie zuweisen, legen Sie auch die Optionen für die Vererbung von Richtlinien fest. Standardmäßig erbt jeder Endpunkt die Richtlinie der übergeordneten Gruppe.
- Richtlinien werden sofort, nachdem sie angelegt oder verändert wurden, per Push an die Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.
- Die Richtlinie bezieht sich nur auf die installierten Sicherheitsmodule.
- Auf der Seite **Richtlinien** werden nur die folgenden Arten von Richtlinien angezeigt:
 - Von Ihnen erstellte Richtlinien

- Andere Richtlinien (z. B. die Standardrichtlinie oder von anderen Benutzern erstellte Vorlagen), die Endpunkten unter Ihrem Konto zugewiesen sind
- Sie können Richtlinien, die von anderen Benutzern erstellt wurden, nicht bearbeiten (es sei denn, der Ersteller der entsprechenden Richtlinie lässt dies in den Richtlinieneinstellungen zu), Sie können sie jedoch außer Kraft setzen, indem Sie den Zielobjekten eine andere Richtlinie zuweisen.



Warnung

Nur die unterstützten Richtlinienmodule werden auf den entsprechenden Endpunkten angewendet.

Bitte beachten Sie, dass für Server-Betriebssysteme nur das Malware-Schutz-Modul unterstützt wird.

7.1. Policies verwalten

Auf der **Richtlinien**-Seite können Sie die Richtlinien einsehen und verwalten.

Richtlinienname	Erstellt von	Geändert am	Ziele	Angewendet / Ausstehend
<input type="checkbox"/> Standard-Richtlinie (Standard)	admin		0	3/ 0

Die Richtlinienübersicht

Jede Art von Endpunkt hat bestimmte Richtlinieneinstellungen. Um Richtlinien zu verwalten, müssen Sie zuerst die Art des Endpunkts (**Computer und Virtuelle Maschinen** oder **Mobilgeräte**) aus der **Ansichtsauswahl** auswählen.

Bestehende Richtlinien werden in der Tabelle angezeigt. Sie können das Folgende für jede Richtlinie einsehen:

- Richtlinienname.
- Benutzer, der die Richtlinie angelegt hat.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde.
- Die Anzahl der Ziele, an die die Richtlinie gesendet wurde.*
- Die Anzahl der Ziele, auf denen die Richtlinie angewendet wurde bzw. die Anwendung noch aussteht.*

Für die Richtlinien bei aktiviertem NSX-Modul stehen weitere Informationen zur Verfügung.

- Der Name der NSX-Richtlinie, der zur Identifizierung der Bitdefender-Richtlinie in VMware vSphere dient.
- Sichtbarkeit der Richtlinie in den Verwaltungskonsolen, ermöglicht Ihnen das Filtern der Richtlinien für NSX. Dementsprechend werden **lokale** Richtlinien ausschließlich in der Bitdefender Control Center angezeigt, während **globale** Richtlinien auch in VMware NSX sichtbar sind.

Diese Details werden standardmäßig ausgeblendet.

So passen Sie die Richtliniendetails an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **III Spalten** auf der rechten Seite der **Symbolleiste**.
2. Wählen Sie die Spalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um zur Standardansicht zurückzukehren.

* Durch Anklicken der Zahl gelangen Sie zur Anzeige der entsprechenden Endpunkte zurück auf die **Netzwerk**-Seite. Wählen Sie bitte **Netzwerkansicht**. Hierdurch wird unter Berücksichtigung der Richtlinien ein **Filter** generiert.


Sie können die bestehenden Richtlinien **sortieren** und über auswählbare Kriterien nach bestimmten Richtlinien **suchen**.

7.1.1. Richtlinien erstellen

Sie können Richtlinien entweder durch Hinzufügen einer neuen oder Duplizieren (Cloning) einer bestehenden Richtlinie erzeugen.

Sicherheitsrichtlinien erstellen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie in der **Ansichtsauswahl** den gewünschten Endpunkttyp.
3. Wählen Sie die Art der Richtlinienerstellung:
 - **Neue Richtlinie hinzufügen.**
 - Klicken Sie auf die Schaltfläche **⊕Hinzufügen** am oberen Ende der Tabelle. Hierüber können Sie ausgehend von der Standardrichtlinienvorlage eine neue Richtlinie erstellen.
 - **Bestehende Richtlinie klonen.**

- a. Markieren Sie das Kästchen der Richtlinie, die Sie klonen möchten.
 - b. Klicken Sie auf die Schaltfläche  **Klonen** am oberen Rand der Tabelle.
4. Konfigurieren Sie die Richtlinieneinstellungen. Detaillierte Informationen finden Sie unter:
- „Richtlinien für Computer und virtuelle Maschinen“ (S. 244)
 - „Richtlinien für Mobilgeräte“ (S. 410)
5. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen und zur Liste der Richtlinien zurückzukehren.

Bei der Definition von Richtlinien zur Anwendung in VMware NSX müssen Sie nicht nur die Einstellungen zum Schutz vor Malware in GravityZone Control Center konfigurieren, sondern auch eine Richtlinie in NSX anlegen und sie anweisen, die GravityZone-Richtlinie als Dienstprofil zu verwenden. So können Sie eine NSX-Sicherheitsrichtlinie anlegen:

1. Melden Sie sich beim vSphere Web Client an.
2. Wechseln Sie zum Reiter **Netzwerk & Sicherheit > Service Composer > Sicherheitsrichtlinien**
3. Klicken Sie in der Symbolleiste über der Richtlinientabelle auf **Sicherheitsrichtlinie anlegen**. Das Konfigurationsfenster wird geöffnet.
4. Geben Sie den Namen der Richtlinie ein und klicken Sie auf **Weiter**.
Sie können optional auch eine kurze Beschreibung hinzufügen.
5. Klicken Sie oben in der Tabelle auf die Schaltfläche **Guest Introspection-Dienst hinzufügen**. Das Fenster für die Konfiguration des Guest Introspection-Dienstes wird angezeigt.
6. Geben Sie den Namen und die Beschreibung des Dienstes ein.
7. Bleibt die Standardaktion ausgewählt, können die Bitdefender-Dienstprofile auf die Sicherheitsgruppe angewendet werden.
8. Wählen Sie im Menü **Dienstname Bitdefender** aus.
9. Wählen Sie im Menü **Dienstprofil** eine bestehende GravityZone-Sicherheitsrichtlinie aus.
10. Verändern Sie die Standardwerte der Optionen **Zustand** und **Erzwingen**.

**Beachten Sie**

Weitere Informationen zu den Einstellungen für die Sicherheitsrichtlinien finden Sie in der [VMware-NSX-Dokumentation](#).

11. Klicken Sie **OK**, um den Dienst hinzuzufügen.

12. Klicken Sie bis zum letzten Schritt auf **Weiter** und klicken Sie danach auf **Fertig stellen**.

7.1.2. Richtlinien zuweisen

Endpunkten wird zunächst die Standardrichtlinie zugewiesen. Nach Definition der erforderlichen Richtlinien auf der **Richtlinien**-Seite können Sie sie den Endpunkten zuweisen.

Der Prozess für die Richtlinienzuordnung ist gebunden an die verschiedenen Umgebungen mit denen GravityZone integriert werden kann. Für gewisse Integrationen, so zum Beispiel mit VMware NSX, kann auf die Richtlinien außerhalb von GravityZone Control Center zugegriffen werden. Sie werden auch externe Richtlinien genannt.

Zuweisung von lokalen Richtlinien

Es gibt zwei Möglichkeiten zur Zuordnung von lokalen Richtlinien:

- **Gerätebasierte Zuweisung** ermöglicht die manuelle Auswahl der gewünschten Endpunkte zur Zuweisung von Richtlinien. Diese Richtlinien werden auch Geräte Richtlinien genannt.
- **Regelbasierte Zuweisung** ermöglicht die Zuweisung einer Richtlinie zu einem verwalteten Endpunkt, wenn die Netzwerkeinstellungen des Endpunkts mit den Bedingungen einer bestehenden Zuweisungsregel übereinstimmen.

**Beachten Sie**

- Sie können nur Richtlinien zuweisen, die auch von Ihnen erstellt wurden. Um eine Richtlinie zuzuweisen, die von einem anderen Benutzer erstellt wurde, müssen Sie sie zunächst auf der Seite **Richtlinien** klonen.
- Auf mit HVI geschützten virtuellen Maschinen können Sie ausschließlich Geräte Richtlinien zuweisen. Wurde auch Bitdefender Endpoint Security Tools installiert, können Sie auch regelbasierte Richtlinien zuweisen, der Sicherheitsagent verwaltet die Richtlinienaktivierung.

Geräterichtlinien zuweisen

In GravityZone lassen sich Richtlinien auf verschiedene Weisen zuweisen:

- Direkte Zuweisung der Richtlinie zum Ziel.
- Zuweisung der Richtlinie zur übergeordneten Gruppe mittels Vererbung.
- Richtlinienvererbung auf das Ziel erzwingen.

Standardmäßig erbt jeder Endpunkt oder Gruppe von Endpunkten die Richtlinie der übergeordneten Gruppe. Wenn Sie die Richtlinie der übergeordneten Gruppe ändern, sind alle untergeordneten Elemente betroffen, mit Ausnahme derjenigen mit einer erzwungenen Richtlinie.

So können Sie eine Geräterichtlinie zuweisen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die Netzwerkansicht aus der [Ansichtsauswahl](#).
3. Wählen Sie die Zielendpunkte aus. Sie können einen oder mehrere Endpunkte oder Gruppen von Endpunkten auswählen.

Aus Vererbungsgründen können Sie die Standardrichtlinie für die Stammgruppe nicht verändern. **Computer und virtuelle Maschinen** wird zum Beispiel immer die **Standardrichtlinie** zugewiesen haben.

4. Klicken Sie auf die Schaltfläche  **Richtlinie zuweisen** am oberen Rand der Tabelle, oder wählen Sie die Option **Richtlinie zuweisen** aus dem Kontextmenü.

Die Seite **Richtlinienzuweisung** wird angezeigt:

Richtlinienzuweisung
✕

Optionen

Die folgende Richtlinienvorlage zuweisen Default policy ▾
 Von oben erben

Richtlinienvererbung für Objekte erzwingen ⓘ

Ziele

Entität	Richtlinie	Geerbt von
Benutzerdefinierte Gruppen	Default policy	Computer und virtuelle Maschinen

Erste Seite
← Seite von 1
→ Letzte Seite
1 Objekt(e)

Fertigstellen
Abbrechen

Einstellungen für die Richtlinienzuweisung

5. Überprüfen Sie die Tabelle mit den Zielpunkten. Für jeden Endpunkt können Sie Folgendes anzeigen:
 - Die zugewiesene Richtlinie.
 - Die übergeordnete Gruppe, von der das Ziel die Richtlinie erbt, falls zutreffend. Wenn die Gruppe die Richtlinie erzwingt, können Sie auf ihren Namen klicken, um die Seite **Richtlinienzuweisung** mit dieser Gruppe als Ziel anzuzeigen.
 - Den Erzwingungsstatus. Dieser Status zeigt an, ob das Ziel die Richtlinienvererbung erzwingt oder gezwungen wird, die Richtlinie zu erben. Beachten Sie die Ziele mit erzwungener Richtlinie (Status **Wird gezwungen**). Ihre Richtlinien können nicht ersetzt werden. In solchen Fällen wird eine Warnmeldung angezeigt.
6. Wird eine Warnung angezeigt, klicken Sie zum Fortfahren auf den Link **Diese Ziele ausschließen**.
7. Wählen Sie eine der verfügbaren Optionen zur Zuordnung der Richtlinie aus:

- **Die folgende Richtlinienvorlage zuweisen** - um den Zielpunkten eine bestimmte Richtlinie direkt zuzuweisen.
 - **Von oben erben** - um die Richtlinie der übergeordneten Gruppe zu verwenden.
8. Wenn Sie sich für die Zuweisung einer Richtlinienvorlage entscheiden:
- a. Wählen Sie die Richtlinie aus der Dropdown-Liste aus.
 - b. Wählen Sie **Richtlinienvererbung auf untergeordnete Gruppen erzwingen**, um Folgendes zu erreichen:
 - Ausnahmslose Zuordnung der Richtlinie zu allen untergeordneten Elementen der Zielgruppen.
 - Verhindern, dass sie von untergeordneter Stelle in der Hierarchie aus geändert wird.

Eine neue Tabelle wird angezeigt, in der rekursiv alle betroffenen Endpunkte und Endpunktgruppen sowie die zu ersetzenden Richtlinien angezeigt werden.

9. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern und zu übernehmen. Klicken Sie andernfalls auf **Zurück** oder **Abbrechen**, um zur vorherigen Seite zurückzukehren.

Nach Abschluss werden die Richtlinien sofort per Push auf die Zielpunkte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Endpunkten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Endpunkt offline ist, werden die Einstellungen übernommen, sobald er wieder online ist.

So überprüfen Sie, ob die Richtlinie erfolgreich zugewiesen wurde:

1. Klicken Sie auf der Seite **Netzwerk** auf den Namen des Endpunktes, den Sie überprüfen möchten. Control Center zeigt das Fenster **Informationen** an.
2. Im Bereich **Richtlinie** können Sie den Status der aktuellen Richtlinie einsehen. Hier muss **Angewendet** angezeigt werden.

Des Weiteren kann der Zuweisungsstatus auch über die Richtliniendetails eingesehen werden:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Finden Sie die Richtlinie, die Sie zugewiesen haben.

In der Spalte **Aktiv/Angewendet/Ausstehend** wird die Anzahl der Endpunkte mit dem jeweiligen Status angezeigt.

3. Wenn Sie auf eine dieser Zahlen klicken, wird eine Liste mit den Endpunkten, die diesen Status haben, auf der Seite **Netzwerk** angezeigt.

Regelbasierte Richtlinien zuweisen

Auf der Seite **Richtlinien > Zuweisungsregeln** können Sie benutzer- oder standortbezogene Richtlinien zu definieren. So können Sie zum Beispiel strengere Firewall-Regeln anwenden, wenn Benutzer außerhalb des Unternehmens eine Internetverbindung herstellen, oder die Internet-Zugangssteuerung für Benutzer aktivieren, die nicht zur Administratorengruppe gehören.

Was Sie über Zuweisungsregeln wissen sollten:

- Endpunkte können jeweils nur eine aktive Richtlinie haben.
- Eine per Regel angewandte Richtlinie überschreibt die am Endpunkt festgelegte Geräterichtlinie.
- Falls keine Zuweisungsregel anwendbar ist, wird die Geräterichtlinie angewandt.
- Regeln werden nach Priorität geordnet und verarbeitet, dabei stellt 1 die höchste Priorität dar. Sie können mehrere Regeln für das gleiche Ziel festlegen. In solchen Fällen wird die erste Regel angewandt, die mit den aktiven Verbindungseinstellungen auf dem Ziel-Endpunkt übereinstimmt.


Stimmt zum Beispiel ein Endpunkt mit einer Benutzerregel mit der Priorität 4 und einer Standortregel mit Priorität 3 überein, kommt die Standortregel zur Anwendung.

Warnung

Stellen Sie sicher, dass beim Erstellen von Regeln sensible Einstellungen wie Ausschlüsse, Kommunikations- oder Proxy-Details berücksichtigt werden.

Als Vorgehensweise wird Richtlinienvererbung empfohlen, um kritische Einstellungen aus der Geräterichtlinie auch in die Richtlinie für Zuweisungsregeln zu übernehmen.

Eine neue Regel generieren:


1. Gehen Sie zur Seite **Zuweisungsregeln**.
2. Klicken Sie auf die Schaltfläche  **Hinzufügen** am oberen Ende der Tabelle.
3. Wählen Sie den Regeltyp aus:
 - **Standortregel**
 - **Benutzerregel**

- **Tag-Regel**

4. Konfigurieren Sie die Regeleinstellungen nach Bedarf.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und die Regel auf den Ziel-Endpunkten für die Richtlinie anzuwenden.

Ändern der Einstellungen einer bestehenden Regel:

1. Suchen Sie auf der Seite **Zuweisungsregeln** nach der entsprechenden Regel und klicken Sie auf ihren Namen, um sie zu bearbeiten.
2. Konfigurieren Sie die Regeleinstellungen nach Bedarf.
3. Klicken Sie auf **Speichern**, um die Änderungen anzuwenden und das Fenster zu schließen. Wenn Sie das Fenster verlassen wollen, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Wenn Sie eine bestimmte Regel nicht mehr verwenden möchten, wählen Sie sie aus und klicken Sie dann am oberen Rand der Tabelle auf die Schaltfläche  **Löschen**. Sie werden aufgefordert, den Vorgang zu bestätigen, indem Sie auf **Ja** klicken.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf  **Neu laden**.

Standortregeln konfigurieren

Ein Standort ist ein Netzwerksegment, das durch eine oder mehrere Netzwerkeinstellungen identifiziert wird, so zum Beispiel ein bestimmtes Gateway, ein bestimmtes DNS, das zu Auflösung von URLs verwendet wird, oder ein IP Subset. Sie können zum Beispiel Standorte wie das LAN des Unternehmens, die Serverfarm oder eine bestimmte Abteilung definieren.

Gehen Sie im Fenster für die Regelkonfiguration folgendermaßen vor:

1. Geben Sie einen passenden Namen und eine Beschreibung der von Ihnen zu erstellenden Regel ein.
2. Legen Sie die Priorität für die Regel fest. Regeln sind nach Priorität geordnet, wobei die erste Regel die höchste Priorität hat. Die gleiche Priorität kann nicht zwei- oder mehrfach vergeben werden.
3. Wählen Sie die Richtlinie aus, für die Sie eine Zuweisungsregel erstellen.
4. Definieren Sie die Standorte, für die die Regel gelten soll.

- a. Wählen Sie den gewünschten Typ aus den Netzwerkeinstellungen im Menu oben in der Standort-Tabelle aus. Die folgenden Typen sind verfügbar:

Typ	Wert
IP/IP-Adressbereich	Bestimmte IP-Adressen in einem Netzwerk oder in Subnetzwerken. Verwenden Sie für Subnetzwerke das CIDR-Format. Zum Beispiel: 10.10.0.12 or 10.10.0.0/16
Gateway-Adresse	IP-Adresse des Gateway
NTP-Server-Adresse	IP-Adresse des WINS-Servers  Wichtig Diese Option gilt nicht für Linux- und Mac-Systeme.
DNS-Server-Adresse	IP-Adresse des DNS-Servers
DNS-Endung der DHCP-Verbindung	DNS-Name ohne den Hostnamen für eine bestimmte DHCP-Verbindung Zum Beispiel: hq.company.biz
Endpunkt kann Host auflösen	Hostname. Zum Beispiel: fileserv.company.biz
Endpunkt kann Verbindung zu GravityZone herstellen	Ja/Nein
Netzwerktyp	Wireless/Ethernet Wenn Sie sich für Wireless entscheiden, können Sie zudem die Netzwerk-SSID hinzufügen.  Wichtig Diese Option gilt nicht für Linux- und Mac-Systeme.
Hostname	Hostname Zum Beispiel: cmp.bitdefender.com

Typ	Wert
	<div style="display: flex; align-items: center;"> <div> <p>Wichtig</p> <p>Sie können auch Platzhalter verwenden. Das Sternchen (*) ersetzt null oder mehr Zeichen und das Fragezeichen (?) ersetzt genau ein Zeichen. Beispiele:</p> <p>*.bitdefender.com</p> <p>cmp.bitdefend???.com</p> </div> </div>

- b. Wert des gewählten Typs eingeben. Sie können gegebenenfalls mehrere Werte in das vorgesehene Feld eingeben; diese werden durch ein Semikolon (;) ohne Leerzeichen getrennt. Wenn Sie zum Beispiel 10.10.0.0/16;192.168.0.0/24 eingeben, gilt die Regel für Ziel-Endpunkte mit einer IP, die auf ALLE diese Subnetzwerke zutrifft.

Warnung Sie können nur eine Netzwerkeinstellungstyp pro Standortregel festlegen. Wenn Sie beispielsweise einen Standort über die **IP/Netzwerkpräfix** hinzugefügt haben, können Sie diese Einstellung in derselben Regel nicht noch einmal verwenden.

- c. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.

Die Netzwerkeinstellungen auf den Endpunkten müssen mit ALLEN angegebenen Standorten übereinstimmen, damit die Regel auf sie angewandt werden kann. Man kann zum Beispiel das LAN-Netzwerk im Büro durch Eingabe des Gateways, Netzwerktyps und DNS identifizieren; darüber hinaus können Sie durch Hinzufügen eines Subnetzwerks eine Abteilung innerhalb des Büro-LANs zu identifizieren.

Standortregel		
Aufenthaltsorte		
IP/Netzwerk-Präfix		
Typ	Wert	Aktionen
IP/Netzwerk-Präfix	10.10.0.0/16;192.168.0.0/24	
Gateway-Adresse	10.10.0.1;192.168.0.1	

Standortregel

Klicken Sie das Feld **Wert** an, um die bestehenden Kriterien zu bearbeiten, und drücken Sie dann zum Speichern auf **Eingabe**.

Um einen Standort zu entfernen, wählen Sie ihn aus und klicken Sie auf **Löschen**.

5. Sie möchten möglicherweise bestimmte Standorte von einer Regel ausschließen. Um eine Ausnahme anzulegen, definieren Sie die Standorte, die von der Regel ausgenommen werden sollen:
 - a. Markieren Sie das Kästchen **Ausschlüsse** unter der Standort-Tabelle.
 - b. Wählen Sie den gewünschten Typ aus den Netzwerkeinstellungen im Menü oben in der Ausschlüsse-Tabelle aus. Weitere Informationen zu den Optionen finden Sie unter „[Standortregeln konfigurieren](#)“ (S. 236).
 - c. Wert des gewählten Typs eingeben. Sie können mehrere Werte in das vorgesehene Feld eingeben; diese werden durch ein Semikolon (;) ohne Leerzeichen getrennt.
 - d. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.

Damit die Ausschlüsse angewandt werden können, müssen die Netzwerkeinstellungen ALLEN in der Ausschlüsse-Tabelle angegebenen Bedingungen erfüllen.

Klicken Sie das Feld **Wert** an, um die bestehenden Kriterien zu bearbeiten, und drücken Sie dann zum Speichern auf **Eingabe**.

Um einen Ausschluss zu entfernen, klicken Sie auf die Schaltfläche **Löschen** am rechten Rand der Tabelle.

6. Klicken Sie auf **Speichern**, um die Zuweisungsregel zu speichern und anzuwenden.

Nachdem eine Standortregel erstellt wurde, wird sie automatisch auf alle verwalteten Ziel-Endpunkte angewandt.

Benutzerregeln konfigurieren



Wichtig

- Sie können nur dann Nutzerregeln erstellen, wenn eine Active-Directory-Integration verfügbar ist.
- Sie können Benutzerregeln ausschließlich für Active-Directory-Benutzer und -Gruppen definieren. Regeln, die auf Active-Directory-Gruppen basieren, werden auf Linux-Computern nicht unterstützt.

Gehen Sie im Fenster für die Regelkonfiguration folgendermaßen vor:

1. Geben Sie einen passenden Namen und eine Beschreibung der von Ihnen zu erstellenden Regel ein.
2. Priorität festlegen. Regeln sind nach Priorität geordnet, wobei die erste Regel die höchste Priorität hat. Die gleiche Priorität kann nicht zwei- oder mehrfach vergeben werden.
3. Wählen Sie die Richtlinie aus, für die Sie eine Zuweisungsregel erstellen.
4. Wählen Sie im Bereich **Ziele** diejenigen Benutzer und Sicherheitsgruppen aus, für die die Richtlinienregel gelten soll. In der Tabelle rechts finden Sie Ihre Auswahl.
5. Klicken Sie auf **Speichern**.

Nachdem eine benutzerorientierte Regeln erstellt wurde, wird sie nach Anmeldung des Benutzers auf die verwalteten Ziel-Endpunkte angewandt.

Konfigurieren von Tag-Regeln



Wichtig

- Sie können nur dann Tag-Regeln erstellen, wenn eine Amazon-EC2- oder eine Microsoft-Azure-Integration vorhanden ist.

Mit den in der Cloud-Infrastruktur definierten Tags können Sie eine bestimmte GravityZone-Richtlinie Ihren in der Cloud gehosteten virtuellen Maschinen zuweisen.

Auf alle virtuellen Maschinen mit den in der Tag-Regel festgelegten Tags wird dann die durch die Regel vorgegebene Richtlinie angewendet.

Beachten Sie

Je nach Cloud-Infrastruktur können Sie die Tags für die virtuellen Maschinen wie folgt definieren:


- Für Amazon EC2: im Reiter **Tags** der EC2-Instanz.
- Für Microsoft Azure: im Bereich **Überblick** der virtuellen Maschine.

Eine Tag-Regel kann ein oder mehrere Tags beinhalten. So erstellen Sie eine Tag-Regel:

1. Geben Sie einen passenden Namen und eine Beschreibung der von Ihnen zu erstellenden Regel ein.
2. Legen Sie die Priorität für die Regel fest. Regeln sind nach Priorität geordnet, wobei die erste Regel die höchste Priorität hat. Die gleiche Priorität kann nicht zwei- oder mehrfach vergeben werden.
3. Wählen Sie die Richtlinie aus, für die Sie die Tag-Regel erstellen möchten.
4. Fügen Sie in der **Tag**-Tabelle einen oder mehrere Tags hinzu.

Ein Tag besteht aus einem Schlüssel/Wert-Paar (Groß-/Kleinschreibung beachten). Achten Sie darauf, die Tags so einzugeben, wie sie in Ihrer Cloud-Infrastruktur definiert sind. Es werden nur gültige Schlüssel/Wert-Paare berücksichtigt.

So fügen Sie einen Tag hinzu:

- a. Geben Sie im Feld **Tag-Schlüssel** den Schlüsselnamen ein.
- b. Geben Sie im Feld **Tag-Wert** den Namen des Werts ein.
- c. Klicken Sie auf die Schaltfläche  **Hinzufügen** auf der rechten Seite der Tabelle.

Zuweisung von NSX-Richtlinien

In NSX werden Sicherheitsrichtlinien Sicherheitsgruppen zugewiesen. Eine Sicherheitsgruppe kann verschiedene vCenter-Objekte enthalten, so zum Beispiel Rechenzentren, Cluster und virtuelle Maschinen.

So können Sie eine Sicherheitsrichtlinie einer Sicherheitsgruppe zuweisen:

1. Melden Sie sich beim vSphere Web Client an.
2. Rufen Sie **Netzwerk & Sicherheit > Service Composer** auf und wechseln Sie zum Reiter **Sicherheitsgruppen**.
3. Legen Sie die benötigte Anzahl an Sicherheitsgruppen an. Weitere Informationen finden Sie in der [VMware-Dokumentation](#).
Sie können dynamische Sicherheitsgruppen auf Grundlage der Sicherheits-Tags anlegen. Auf diese Weise können Sie alle als infiziert erkannten virtuellen Maschinen gruppieren.
4. Klicken Sie mit der rechten Maustaste auf die Sicherheitsgruppe, für die sich interessieren und klicken Sie auf **Richtlinie anwenden**.
5. Wählen Sie die anzuwendende Richtlinie aus und klicken Sie auf **OK**.

7.1.3. RichtlinienEinstellungen ändern

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.



Beachten Sie

Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

So ändern Sie die Einstellungen einer bestehenden Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie in der [Ansichtsauswahl](#) den gewünschten Endpunkttyp.
3. Finden Sie die Richtlinie in der Liste, und klicken Sie auf ihren Namen, um sie zu bearbeiten.
4. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Detaillierte Informationen finden Sie unter:
 - [„Richtlinien für Computer und virtuelle Maschinen“ \(S. 244\)](#)
 - [„Richtlinien für Mobilgeräte“ \(S. 410\)](#)
5. Klicken Sie auf **Speichern**.

Richtlinien werden sofort nach einer Änderung der Richtlinienzuweisung oder der Richtlinieneinstellungen per Push an die entsprechenden Netzwerkobjekte

übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.

7.1.4. Richtlinien umbenennen

Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.

Um eine Richtlinie umzubenennen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie in der **Ansichtsauswahl** den gewünschten Endpunkttyp.
3. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinienseite.
4. Geben Sie einen neuen Namen für die Richtlinie ein.
5. Klicken Sie auf **Speichern**.



Beachten Sie

Jeder Richtliniename ist einzigartig. Sie müssen für jede Richtlinie einen eigenen Namen eingeben.

7.1.5. Richtlinien löschen

Löschen Sie eine Richtlinie, wenn Sie sie nicht mehr länger benötigt wird. Nach dem Löschen der Richtlinie wird den Netzwerkobjekten, auf die sie zuvor angewendet wurde, die Richtlinie der übergeordneten Gruppe zugewiesen. Sollte keine andere Richtlinie angewendet werden, wird zwangsläufig die Standardrichtlinie übernommen. Wenn eine Richtlinie gelöscht wird, die von einer anderen Richtlinie geerbte Bereiche enthält, werden die Einstellungen der geerbten Bereiche auf den untergeordneten Richtlinien gespeichert.



Beachten Sie

Standardmäßig kann nur der Benutzer eine Richtlinie löschen, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Um eine NSX-Richtlinie aus der GravityZone Control Center löschen zu können, müssen Sie zunächst sicherstellen, dass die Richtlinie nicht genutzt wird. Weisen

Sie der gewünschten Sicherheitsgruppe daher ein anderes Sicherheitsprofil zu. Weitere Informationen finden Sie unter „Zuweisung von NSX-Richtlinien“ (S. 241).

Um eine Richtlinie zu löschen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie in der **Ansichtsauswahl** den gewünschten Endpunkttyp.
3. Markieren Sie das Kästchen der Richtlinie, die Sie löschen möchten.
4. Klicken Sie auf die Schaltfläche **☒ Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

7.2. Richtlinien für Computer und virtuelle Maschinen

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.

So konfigurieren Sie die Einstellungen einer Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinieneinstellungsseite
4. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Die Einstellungen sind in die folgenden Bereiche eingeteilt:
 - [Allgemein](#)
 - [HVI](#)
 - [Malware-Schutz](#)
 - [Sandbox Analyzer](#)
 - [Firewall](#)
 - [Netzwerkschutz](#)
 - [Patch-Verwaltung](#)
 - [Anwendungssteuerung](#)
 - [Gerätesteuerung](#)
 - [Relais](#)
 - [Exchange-Schutz](#)
 - [Verschlüsseln](#)
 - [NSX](#)
 - [Speicherschutz](#)

Durchsuchen Sie die Bereich über das Menü links auf der Seite.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und auf die Ziel-Computer anzuwenden. Wenn Sie die Richtlinienseite verlassen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.



Beachten Sie

Wie Sie Richtlinien verwenden, erfahren Sie unter „[Policies verwalten](#)“ (S. 228).

7.2.1. Allgemein

Mithilfe der allgemeinen Einstellungen können Sie für die entsprechenden Endpunkte Anzeigeeinstellungen, Proxy-Einstellungen, Power-User-Einstellungen, Kommunikationsoptionen und Update-Einstellungen konfigurieren.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [Details](#)
- [Benachrichtigungen](#)
- [Einstellungen](#)
- [Kommunikationsserver](#)
- [Update \(Aktualisierung\)](#)

Details

Auf der Seite **Details** finden Sie allgemeine Informationen zu den Richtlinien:

- Richtliniename
- Benutzer, der die Richtlinie angelegt hat
- Datum und Zeitpunkt, zu dem die Richtlinie erstellt wurde.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde

Herzlich willkommen, Admin

Allgemein

Details

Benachrichtigungen

Einstellungen

Kommunikation

Update

Malware-Schutz

Richtliniendetails

Name: *

Anderen Benutzern erlauben, diese Richtlinie zu ändern

Verlauf

Erstellt von:

Erstellt am:

Richtlinien für Computer und virtuelle Maschinen

Sie können die Richtlinie umbenennen, indem Sie den neuen Namen in das entsprechende Feld eingeben und unten auf der Seite auf die Schaltfläche **Speichern** klicken. Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.



Beachten Sie

Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Vererbungsregeln

Sie können Bereiche auswählen, die von anderen Richtlinien ererbt werden sollen. Dazu müssen Sie:

1. Das Modul und den Bereich auswählen, die an die aktuelle Richtlinie vererbt werden sollen. Alle Bereiche sind vererbbar außer **Allgemein > Details**.
2. Spezifizieren Sie die Richtlinie, von der Sie den Bereich vererben wollen.
3. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle.

Falls die Quellrichtlinie gelöscht wird, endet die Vererbung und die Einstellungen des vererbten Bereichs werden in der Zielrichtlinie gespeichert.

Vererbte Bereiche können nicht an andere Richtlinien weitervererbt werden. Hierzu ein Beispiel:

Richtlinie A erbt den Bereich **Malware-Schutz > Bei Bedarf** von Richtlinie B. Richtlinie C kann den Bereich **Malware-Schutz > Bei Bedarf** nicht von Richtlinie A erben.

Informationen zum technischen Support

Durch Ausfüllen der entsprechenden Felder können Sie die im **Über**-Fenster des Sicherheitsagenten angezeigten Informationen zum technischen Support und Kontaktdaten selbst anpassen.

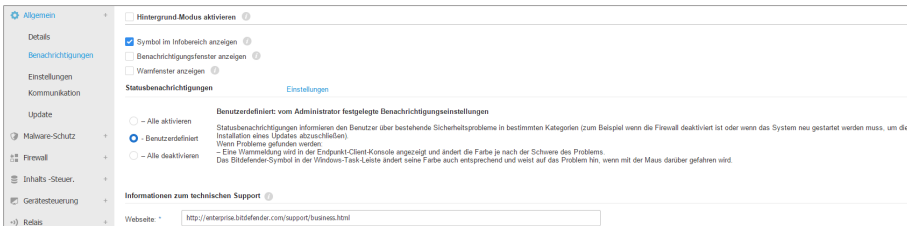
Damit die Standard-E-Mail-Anwendung auf dem Endpunkt geöffnet wird, wenn man im Bereich **Über** auf die E-Mail-Adresse klickt, müssen Sie sie im Feld **E-Mail** mit dem Präfix "mailto:" hinzufügen. Beispiel: `mailto: name@domain.com`.

Benutzer können auf diese Informationen aus der Konsole des Sicherheitsagenten zugreifen, indem sie mit der rechten Maustaste auf das **B** Bitdefender-Symbol in der Task-Leiste klicken und anschließend **Über** wählen.

Benachrichtigungen

In diesem Bereich können Sie die Anzeigeeoptionen für die Benutzeroberfläche des Bitdefender-Sicherheitsagenten einfach und bequem konfigurieren.

Mit nur einem Klick können Sie bestimmte Benachrichtigungstypen vollständig aktivieren oder deaktivieren, um nur die für Sie wichtigen Informationen zu erhalten. Auf der gleichen Seite können Sie zudem steuern, welche Endpunktprobleme sichtbar sein sollen.



Richtlinien - Anzeigeeinstellungen

- **Hintergrund-Modus.** Über das Kästchen können Sie den Hintergrundmodus ein- und ausschalten. Der Hintergrund-Modus soll Ihnen helfen, Benutzereingriffe in den Sicherheitsagenten einfach zu unterbinden. Bei der Aktivierung des Hintergrund-Modus werden die folgenden Änderungen an der Richtlinienkonfiguration aktiv:

- Die Optionen **Symbol im Infobereich anzeigen**, **Benachrichtigungsfenster anzeigen** und **Warnfenster anzeigen** in diesem Bereich werden deaktiviert.
- Wenn die **Firewall-Sicherheitsstufe** auf **Bestehende Regeln und nachfragen** oder **Bestehende Regeln, bekannte Dateien und nachfragen** eingestellt war, wird jetzt auf **Bestehende Regeln, bekannte Dateien und zulassen** eingestellt. Ansonsten wird die Einstellung der Sicherheitsstufe nicht verändert.
- **Symbol im Infobereich anzeigen.** Wählen Sie diese Option, um das **B** Bitdefender-Symbol im Infobereich (in der Task-Leiste) anzuzeigen. Das Symbol zeigt dem Benutzer den Sicherheitsstatus an, indem es sein Aussehen verändert und ein entsprechendes Benachrichtigungsfenster anzeigt. Außerdem kann der Benutzer mit der rechten Maustaste auf das Symbol klicken, um das Hauptfenster des Sicherheitsagenten oder das **Über**-Fenster zu öffnen.
- **Pop-up-Warnmeldungen anzeigen.** Der Nutzer wird per Warnfenster über Sicherheitsereignisse informiert, die sein Eingreifen erfordern. Wenn Sie Warnfenster nicht anzeigen lassen, führt der Sicherheitsagent automatisch die empfohlene Aktion aus. Warnfenster werden in den folgenden Situationen angezeigt:
 - Wenn die Firewall so konfiguriert ist, dass der Benutzer entscheidet, welche Aktion ausgeführt wird, wenn unbekannte Anwendungen auf Netzwerk oder Internet zugreifen wollen.
 - Wenn Advanced Threat Control/Angriffserkennungssystem aktiviert wird, wenn eine potenziell schädliche Anwendung gefunden wird.
 - Wenn der Geräte-Scan aktiviert ist und ein externes Speichermedium an den Computer angeschlossen wird. Diese Einstellung kann unter **Malware-Schutz > Bei Bedarf** vorgenommen werden.
- **Benachrichtigungsfenster anzeigen.** Anders als Warnfenster informieren Benachrichtigungsfenster den Nutzer über verschiedenste Sicherheitsereignisse. Diese Benachrichtigungsfenster werden automatisch nach ein paar Sekunden ausgeblendet, ohne dass der Benutzer etwas tun muss.

Wählen Sie **Benachrichtigungsfenster anzeigen** und klicken Sie danach auf **Modulare Einstellungen anzeigen**, um festzulegen, über welche Ereignisse der Nutzer von den einzelnen Modulen informiert werden soll. Es gibt drei Arten von Benachrichtigungsfenstern, die sich je nach Schwere des Ereignisses unterscheiden:

- **Info.** Der Nutzer wird über wichtige, aber harmlose Sicherheitsereignisse informiert. So zum Beispiel über eine Anwendung, die sich mit dem Internet verbunden hat.
- **Gering.** Der Nutzer wird über wichtige Sicherheitsereignisse informiert, die unter Umständen seine Aufmerksamkeit erfordern könnten. So zum Beispiel, wenn der Zugriff-Scan eine Bedrohung erkannt hat und die Datei in die Quarantäne verschoben wurde.
- **Kritisch.** Diese Benachrichtigungsfenster informieren den Nutzer über gefährliche Situationen, so z. B. wenn der Zugriff-Scan eine Bedrohung erkannt hat und die Standardaktion der Richtlinie **Keine Aktion ausführen** lautet und sich die Malware damit weiterhin auf dem Endpunkt befindet. Ein weiteres Beispiel wäre ein nicht abgeschlossener Updateprozess.

Wählen Sie das dem Typennamen zugeordnete Kästchen aus, um diesen Benachrichtigungstyp für alle Module gleichzeitig zu aktivieren. Klicken Sie auf das dem jeweiligen Modul zugeordnete Kästchen, um bestimmte Benachrichtigungen zu aktivieren oder deaktivieren.

Die angezeigten Module können sich je nach Lizenz unterscheiden.

- **Sichtbarkeit von Endpunktproblemen.** Benutzer werden auf Konfigurationsprobleme in der Sicherheit ihres Endpunktes durch Statusbenachrichtigungen hingewiesen. So werden Benutzer zum Beispiel darauf hingewiesen, wenn ein Problem im Malware-Schutz besteht, zum Beispiel wenn das Zugriff-Scan-Modul deaktiviert ist oder ein vollständiger Systemscan überfällig ist. Benutzer werden über Ihren Schutzstatus auf zwei Wegen informiert:
 - Überprüfen des Statusbereichs des Hauptfensters, welches die entsprechenden Statusmeldungen anzeigt und das je nach Schwere des Sicherheitsproblems die Farbe ändert. Über einen Klick auf die entsprechende Schaltfläche können Benutzer Details zum jeweiligen Problem anzeigen.
 - durch das **B** Bitdefender-Symbol in der Task-Leiste, das sich ändert, wenn Probleme entdeckt werden.

Der Bitdefender-Sicherheitsagent verwendet die folgende Farbcodierung im Infobereich:

- Grün: keine Probleme gefunden.

- **Gelb:** Auf dem Endpunkt gibt es nicht-kritische Probleme mit der Sicherheit. Benutzer müssen ihre Arbeit nicht unbedingt unterbrechen, um diese Probleme zu beheben.
- **Rot:** Auf dem Endpunkt gibt es kritische Probleme, die umgehende Aufmerksamkeit erfordern.

Wählen Sie **Sichtbarkeit von Endpunktproblemen** aus und klicken Sie danach auf **Modulare Einstellungen anzeigen**, um die in der Benutzeroberfläche des Bitdefender Agent angezeigten Statusbenachrichtigungen individuell anzupassen.


Sie können für jedes Modul festlegen, ob die Benachrichtigung als Warnung, als kritisches Problem oder gar nicht angezeigt werden soll. Sie haben diese Optionen:

- **Allgemein.** Eine Statusbenachrichtigung wird ausgegeben, wenn ein Systemneustart während oder nach eines Produktwartungsvorgangs erforderlich wird und auch wenn der Sicherheitsagent keine Verbindung zu Bitdefender Cloud Services herstellen konnte.
- **Malware-Schutz.** In den folgenden Situationen werden Statusbenachrichtigungen ausgegeben:
 - Zugriff-Scans sind aktiviert, aber viele lokale Dateien werden übersprungen.
 - Seit dem letzten vollständigen Systemscan auf der Maschine ist eine bestimmte Anzahl an Tagen verstrichen.
Sie können festlegen, wie die Benachrichtigungen angezeigt werden und wie viele Tage der letzte vollständige Systemscan her sein darf.
 - Zum Abschluss eines Desinfektionsvorgangs muss ein Neustart durchgeführt werden.
- **Firewall.** Diese Statusbenachrichtigung wird ausgegeben, wenn das Firewall-Modul deaktiviert ist.
- **Anwendungssteuerung.** Diese Statusbenachrichtigung wird ausgegeben, wenn Veränderungen im Anwendungssteuerungsmodul vorgenommen werden.
- **Inhaltssteuerung.** Diese Statusbenachrichtigung wird ausgegeben, wenn das Inhaltssteuerungsmodul deaktiviert ist.

- **Update.** Die Statusbenachrichtigung wird immer dann ausgegeben, wenn ein Systemneustart durchgeführt werden muss, um einen Update-Vorgang abzuschließen.
- **Benachrichtigung über Endpunktneustart.** Mit dieser Option wird auf dem Endpunkt eine Neustartbenachrichtigung angezeigt, wenn ein Systemneustart aufgrund von Änderungen am Endpunkt durch die unter den Moduleinstellungen ausgewählten GravityZone-Module erforderlich ist.



Beachten Sie

Endpunkte, die einen Systemneustart erfordern, werden im GravityZone-Inventar mit einem entsprechenden Statussymbol () angezeigt.

Sie können die Neustartbenachrichtigungen weiter anpassen, indem Sie auf **Modulare Einstellungen anzeigen** klicken. Die folgenden Optionen stehen zur Verfügung:

- **Update** - Wählen Sie diese Option, um Neustartbenachrichtigungen bei Updates des Agenten zu aktivieren.
- **Patch Management** - Wählen Sie diese Option, um Neustartbenachrichtigungen bei Patch-Installationen zu aktivieren.



Beachten Sie

Sie können auch festlegen, für wie viele Stunden ein Benutzer einen Neustart maximal verschieben kann. Wählen Sie dazu **Maschine automatisch neu starten nach** und geben Sie einen Wert von 1 bis 46 ein.

Die Neustartbenachrichtigung fordert den Benutzer auf, eine der folgenden Aktionen auszuwählen:

- **Jetzt neu starten.** Das System wird sofort neu gestartet.
- **Neustart aufschieben.** In diesem Fall wird regelmäßig eine Neustartbenachrichtigung angezeigt, bis der Benutzer das System neu startet oder bis die vom Unternehmensadministrator festgelegte Zeit abgelaufen ist.

Einstellungen

In diesem Bereich können Sie die folgenden Einstellungen konfigurieren:

- **Passwortkonfiguration.** Um zu verhindern, dass Benutzer mit Administratorenrechten den Schutz deinstallieren, müssen Sie ein Passwort festlegen.

Das Deinstallationspasswort kann schon vor der Installation festgelegt werden, indem Sie das Installationspaket individuell anpassen. Falls Sie dies getan haben, wählen Sie **Installationseinstellungen beibehalten**, um das aktuelle Passwort beizubehalten.

Um das Passwort einzurichten oder das aktuelle Passwort zu ändern, wählen Sie **Passwort aktivieren** und geben Sie das gewünschte Passwort ein. Um den Passwortschutz zu entfernen, wählen Sie **Passwort deaktivieren**.

- **Proxy-Konfiguration**

Wenn sich Ihr Netzwerk hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen angeben, mithilfe derer Ihre Endpunkte mit den GravityZone-Komponenten kommunizieren können. In diesem Fall müssen Sie die Option **Proxy-Konfiguration** aktivieren und die entsprechenden Parameter eingeben:

- **Server** - Geben Sie die IP-Adresse des Proxy-Servers ein
- **Port** - Geben Sie den Port ein, über den die Verbindung zum Proxy-Server hergestellt wird.
- **Benutzername** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
- **Passwort** – Geben Sie hier das gültige Passwort für den entsprechenden Benutzer ein.

- **Power-User**

Mit dem Power-User-Modul können Benutzern auf Endpunkt-Ebene Administratorrechte verliehen werden, mit denen diese Benutzer über Bitdefender Endpoint Security Tools Richtlinieneinstellungen anzeigen und verändern können.

Wenn Sie für bestimmte Endpunkte Power-User-Rechte festlegen möchten, müssen Sie dieses Modul zunächst in den Sicherheitsagenten, der auf den entsprechenden Endpunkten installiert ist, integrieren. Danach müssen Sie die Power-User-Einstellungen in der diesen Endpunkten zugewiesenen Richtlinie konfigurieren:



Wichtig

Das Power-User-Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

1. Aktivieren Sie die Option **Power-User**.
2. Legen Sie in den Feldern darunter ein Power-User-Passwort fest.

Benutzer, die von einem lokalen Endpunkt aus in den Power-User-Modus wechseln möchten, werden dann aufgefordert, dieses Passwort einzugeben.

Benutzer können das Power-User-Modul öffnen, indem sie mit der rechten Maustaste auf das **B** Bitdefender-Symbol in ihrer Task-Leiste klicken und dann aus dem Kontextmenü **Power-User** wählen. Nach Eingabe des Passworts im Anmeldefenster wird eine Konsole geöffnet, in der der Benutzer die Richtlinieneinstellungen sehen und ändern kann.



Beachten Sie

Über die Power-User-Konsole kann lokal nur auf bestimmte Sicherheitsfunktionen zugegriffen werden: Malware-Schutz, Firewall, Inhaltssteuerung und Gerätesteuerung.

So können Sie die Änderungen rückgängig machen, die im Power-User-Modus gemacht wurden:

- Öffnen Sie im Control Center die Richtlinienvorlage, die dem Endpunkt mit Power-User-Rechten zugewiesen ist, und klicken Sie auf **Speichern**. So werden die ursprünglichen Einstellungen wieder auf den Endpunkt angewendet.
- Weisen Sie dem Endpunkt mit Power-User-Rechten eine neue Richtlinie zu.
- Melden Sie sich lokal an dem Endpunkt an, öffnen Sie die Power-User-Konsole und klicken Sie auf **Erneut synchronisieren**.

So finden Sie schnell Endpunkte, deren Richtlinien im Power-User-Modus verändert wurden:

- Klicken Sie auf der Seite **Netzwerk** auf das Menü **Filter** und markieren Sie dann im Reiter **Richtlinie** das Kästchen **Bearbeitet vom Power-User**.
- Klicken Sie auf der Seite **Netzwerk** auf den gewünschten Endpunkt um das Fenster **Informationen** zu öffnen. Wenn die Richtlinie im Power-User-Modus verändert wurde, wird im Bereich **Richtlinie** des Reiters **Allgemein** ein Hinweis angezeigt.



Wichtig

Das Power-User-Modul dient in erster Linie zur Fehlerbehebung, denn mit diesem Modul kann der Netzwerkadministrator unkompliziert Richtlinieneinstellungen auf lokalen Computern anzeigen und ändern. Die Vergabe von Power-User-Rechten innerhalb des Unternehmens muss auf befugte Personen beschränkt bleiben, um sicherzustellen, dass die Sicherheitsrichtlinien stets auf alle Endpunkte im Unternehmensnetzwerk angewendet werden.

• Optionen

In diesem Bereich können Sie die folgenden Einstellungen festlegen:

- **Ereignisse entfernen, die älter sind als (Tage).** Bitdefender security agent führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung überwacht werden). Ereignisse werden standardmäßig nach 30 Tagen aus dem Protokoll gelöscht. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Berichte über Systemabstürze an Bitdefender schicken.** Wählen Sie diese Option, damit Berichte zur Analyse an die Bitdefender-Labors geschickt werden, wenn der Sicherheitsagent abstürzt. Die Berichte helfen unseren Mitarbeitern dabei, die Ursache des Problems zu finden und ein Wiederauftreten zu verhindern. Es werden keine persönlichen Informationen mitgesendet.
- **Verdächtige ausführbare Dateien zur Analyse übermitteln.** Wählen Sie diese Option aus, damit nicht vertrauenswürdige oder verdächtige Dateien zur Analyse an die Bitdefender Labs übermittelt werden.
- **HVI-Speicherverletzungen an Bitdefender übermitteln.** HVI übermittelt standardmäßig anonymisierte Daten über erkannte Verletzungen zu Statistikzwecken und zur Verbesserung der Erkennungsraten an die Bitdefender-Cloud-Server. Entfernen Sie das entsprechende Häkchen, wenn Sie diese Daten nicht über Ihr Netzwerk übermitteln möchten.

Kommunikationsserver

In diesem Bereich können Sie den gewünschten Endpunkten eine oder mehrere Relais-Maschinen zuweisen und dann die Proxy-Einstellungen für die Kommunikation zwischen diesen Endpunkten und der GravityZone konfigurieren.

Kommunikationszuweisung für Endpunkte

Wenn auf der GravityZone-Appliance mehrere Kommunikationsserver installiert sind, können Sie den entsprechenden Computern über eine Richtlinie einen oder mehrere Kommunikationsserver zuweisen. Bestehende Relais-Endpunkte, die als Kommunikationsserver dienen, werden mit berücksichtigt.


So weisen Sie Zielcomputern Kommunikationsserver zu:

1. Klicken Sie in der Tabelle **Kommunikationszuweisung für Endpunkte** auf das Feld **Name**. Die Liste der gefundenen Kommunikationsserver wird angezeigt.
2. Wählen Sie eine Entität.

Priorität	Name	Benutzerdefinierter Name/IP	Aktionen
	ECS 192.168.3.71		
	BDVM-PC-TEO		
	WIN-AKORN6RFLUC		

Richtlinien für Computer und virtuelle Maschinen - Kommunikations-Einstellungen

3. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle. Der Kommunikationsserver wird der Liste hinzugefügt. Alle Zielcomputer werden über den angegebenen Kommunikationsserver mit dem Control Center kommunizieren.
4. Wiederholen Sie diese Schritte, um weitere Kommunikationsserver hinzuzufügen, soweit verfügbar.
5. Sie können die Priorität der Kommunikationsserver konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile klicken. Die Kommunikation mit den Zielcomputern läuft über die Entität, die ganz oben in der Liste steht. Sollte die Kommunikation über diese Entität nicht möglich sein, wird es über die nächste in der Liste versucht.

- Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche  **Löschen** auf der rechten Seite der Tabelle.

Kommunikation zwischen Endpunkte und Relais / GravityZone

In diesem Bereich können Sie die Proxy-Einstellungen für die Kommunikation zwischen den Zielendpunkten und den zugewiesenen Relais-Maschinen, bzw. für den Fall, dass kein Relais zugewiesen wurde, zwischen den Zielendpunkten und der GravityZone-Appliance konfigurieren:

- Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.
- Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den GravityZone-Komponenten kommunizieren.

Kommunikation zwischen Endpunkte und Cloud Services

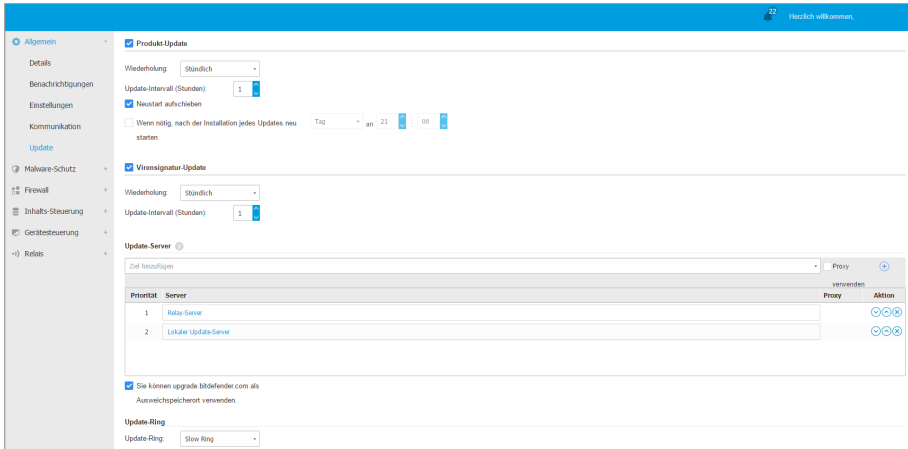
In diesem Bereich können Sie die Proxy-Einstellungen für die Kommunikation zwischen den Zielendpunkten und Bitdefender Cloud Services konfigurieren (eine Internet-Verbindung ist nötig):

- Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.
- Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den GravityZone-Komponenten kommunizieren.

Update (Aktualisierung)

Updates sind von großer Wichtigkeit, da nur so den neuesten Bedrohungen begegnet werden kann. Bitdefender veröffentlicht sämtliche Updates des Produkts oder der Sicherheitsinhalte über die Bitdefender-Server im Internet. Alle Updates sind verschlüsselt und digital signiert, sodass sie nicht verfälscht werden können. Wenn ein neues Update zur Verfügung steht, überprüft der Bitdefender-Sicherheitsagent die digitale Signatur des Updates auf Authentizität und den Inhalt des Pakets auf

Unversehrtheit. Anschließend wird jede Update-Datei geparkt und ihre Version mit der installierten Datei verglichen. Neuere Dateien werden lokal heruntergeladen und mit ihrem MD5-Hashwert verglichen, um sicher zu gehen, dass sie nicht verändert wurden. In diesem Bereich können Sie die Update-Einstellungen für Bitdefender-Sicherheitsagenten und -Sicherheitsinhalte konfigurieren.



Richtlinien für Computer und virtuelle Maschinen - Update-Optionen

- **Produkt-Update.** Der Bitdefender-Sicherheitsagent wird stündlich automatisch nach Updates suchen und diese herunterladen und installieren (Standardeinstellung). Automatische Updates werden unauffällig im Hintergrund durchgeführt.
 - **Wiederholung.** Um die automatische Update-Wiederholung zu ändern, wählen Sie eine andere Option von der Menüleiste und konfigurieren Sie es nach Ihren Bedürfnissen, in den folgenden Feldern.
 - **Neustart aufschieben.** Manche Updates machen einen Neustart des Systems erforderlich, um die Installation abzuschließen. Standardmäßig funktioniert das Produkt mit den alten Dateien weiter, bis der Computer neu gestartet wird. Dann werden die neuesten Updates angewendet. Ansonsten wird eine Benachrichtigung in der Benutzeroberfläche den Benutzer auffordern, das System neu starten, sollte dies wegen eines Updates erforderlich sein. Es wird empfohlen, diese Option aktiviert zu lassen. Sonst wird das System automatisch neu gestartet, wenn ein Update installiert wurde, das einen

Neustart erfordert. Dem Benutzer wird die Gelegenheit gegeben, den aktuellen Arbeitsstand zu speichern, aber der Neustart kann nicht abgebrochen werden.

- Wenn Sie den Zeitpunkt des Neustarts verschieben möchten, können Sie eine passendere Zeit festlegen, zu der die Computer automatisch neu gestartet werden, sollte dies (weiterhin) nötig sein. Dies erweist sich insbesondere bei Servern als sehr nützlich. Klicken Sie auf **Wenn nötig, nach der Installation von Updates neu starten** und legen Sie eine passende Zeit für den Neustart fest (täglich, wöchentlich an einem bestimmten Tag, zu einer bestimmten Uhrzeit).
- **Update der Sicherheitsinhalte.** Sicherheitsinhalte bezeichnet statische und dynamische Mittel zur Erkennung von Bedrohungen, wie, aber nicht beschränkt auf, Scan-Engines, maschinelle Lernmodelle, Heuristiken, Regeln, Signaturen und Blacklists. Der Bitdefender-Sicherheitsagent wird stündlich automatisch nach Updates der Sicherheitsinhalte suchen (Standardeinstellung). Automatische Updates werden unauffällig im Hintergrund durchgeführt. Um die automatische Update-Wiederholung zu ändern, wählen Sie eine andere Option von der Menüleiste und konfigurieren Sie es nach Ihren Bedürfnissen, in den folgenden Feldern.
- **Update-Adressen.** Der Standard-Update-Server des Bitdefender-Sicherheitsagenten ist der lokale GravityZone-Update-Server. Hinzufügen einer Update-Adresse entweder durch Auswahl einer vordefinierte Adresse aus der Auswahlliste oder durch Eingabe des IP- oder Host-Namen eines oder mehrerer Update-Server Ihres Netzwerks. Legen Sie deren Priorität mithilfe der Richtungspfeile fest, die beim Mouseover angezeigt werden. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

Um die lokale Update-Adresse einzurichten:

1. Geben Sie die Adresse des Update-Servers im Feld **Ziel hinzufügen** ein. Sie können:
 - Wählen Sie einen vorgegebenen Speicherort:
 - **Relay-Server.** Der Endpunkt verbindet sich automatisch mit dem ihm zugewiesenen Relay-Server.



Warnung

Relais-Server werden auf veralteten Betriebssystemen nicht unterstützt. Weitere Informationen hierzu finden Sie in der Installationsanleitung.



Beachten Sie

Sie können den zugewiesenen Relay-Server im Fenster **Informationen** einsehen. Weitere Details finden Sie unter [Anzeigen von Computerdetails](#).

- **Lokaler Update-Server**
- Geben Sie die IP-Adresse oder den Host-Namen eines oder mehrerer Update-Server in Ihrem Netzwerk ein. Verwenden Sie dazu eine der folgenden Syntaxoptionen:
 - `update_server_ip:port`
 - `update_server_name:port`



Der Standard-Port ist 7074.

Das Kästchen **Bitdefender-Server als Ausweichadresse verwenden** ist standardmäßig markiert. Falls keine Update-Adressen verfügbar sind, wird die Ausweichadresse verwendet.



Warnung

Durch Deaktivierung der Ausweichadresse werden keine Updates mehr installiert; Ihr Netzwerk wird anfällig, wenn die vorgesehenen Adressen nicht mehr verfügbar sind.

2. Falls sich Client-Computer über einen Proxy-Server mit dem lokalen Update-Server verbinden, aktivieren Sie **Proxy benutzen**.
3. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle.
4. Legen Sie mithilfe der Pfeile  und  in der Spalte **Aktion** die Priorität der definierten Update-Server fest. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende **×** **Löschen**-Schaltfläche. Es ist zwar möglich, die standardmäßige Update-Adresse zu entfernen, dies wird jedoch nicht empfohlen.

- **Update-Ring.** Sie können Produktupdates über die Update-Ringe auch phasenweise ausrollen:
 - **Slow Ring.** Die Computer mit einer Slow-Ring-Richtlinie erhalten die Updates zu einem späteren Zeitpunkt, je nachdem, wie die Rückmeldung der Endpunkte im Fast Ring lautet. Dabei handelt es sich um eine Vorsichtsmaßnahme im Updateprozess. Dies ist die Standardeinstellung.
 - **Fast Ring.** Die Maschinen mit einer Fast Ring-Richtlinie erhalten jeweils die ganz frisch verfügbaren Updates. Diese Einstellung empfiehlt sich für die unkritischen Maschinen in der Produktionsumgebung.



Wichtig

- Für den unwahrscheinlichen Fall, dass im Fast Ring ein Problem auf Computern mit einer bestimmten Konfiguration auftritt, kann es vor dem Slow-Ring-Update behoben werden.
- Staging wird von BEST for Windows Legacy nicht unterstützt. Die Legacy-Endpunkte in der Stagingumgebung müssen in die Produktionsumgebung verschoben werden.



Beachten Sie

Einzelheiten zu den Auswirkungen der Auswahl des jeweiligen Ring-Verfahrens für die Update-Verteilung auf die Bereitstellung entnehmen Sie dem Abschnitt **Aktualisieren von GravityZone > Bereitstellung** in der GravityZone-Installationsanleitung.

7.2.2. HVI



Beachten Sie

HVI bietet nur virtuellen Maschinen auf Citrix Xen-Hypervisoren Schutz.

Hypervisor Memory Introspection schützt virtuelle Maschinen gegen fortschrittliche Bedrohungen, die Signatur-basierte Engines nicht abwehren können. Es stellt Echtzeit-Erkennung von Angriffen sicher, indem es Vorgänge von außerhalb des Gast-Betriebssystems überwacht. Der Schutzmechanismus enthält mehrere Optionen, um Angriffe abzuwehren, sobald sie auftreten, und die Bedrohung sofort zu eliminieren.

Gemäß Speichertrennungs-Prinzip des Betriebssystems enthält HVI zwei Sicherheitsmodule in den zugehörigen Kategorien:

- **Benutzerbereich** für normale Vorgänge aus Benutzeranwendungen.
- **Kernel-Bereich** für Prozesse im Core des Betriebssystems.

Darüber hinaus umfasst die HVI-Richtlinie zwei Funktionen, die Sie bei der Sicherheitsverwaltung und der Verwaltung der geschützten virtuellen Maschinen unterstützen:

- **Ausschlüsse** zum Anzeigen und Verwalten von Prozessen, die von den Scans ausgenommen sind.
- **Benutzerdefinierte Tools** zur Injektion von Tools, die für Betriebs- und Forensikzwecke benötigt werden, in das Gastbetriebssystem.

Benutzerbereich

Hier können Sie die Sicherheitseinstellungen für Vorgänge im Speicher des Benutzerbereichs konfigurieren.

Verwenden Sie das Kontrollfeld **Memory Introspection Benutzerbereich** zum Aktivieren oder Deaktivieren des Schutzes.

Die Funktionalität dieses Moduls hängt von Regeln ab, mit denen der Schutz für unterschiedliche Prozessgruppen separat konfiguriert werden kann. Zusätzlich können weitere forensische Daten gesammelt werden.

- **Benutzerbereich-Regeln**
- **Forensische Informationen**

Benutzerbereich-Regeln

Das Modul enthält einen Satz vordefinierter Regeln für die anfälligsten Anwendungen. Die Tabellen in diesem Bereich listen bestehende Regeln sowie die wichtigsten Informationen zu den einzelnen Regeln auf:

- Name der Regel
- Vorgänge, für die die Regel gilt
- Überwachungsmodus
- Aktion, die den erkannten Angriff abwehrt
- Aktionen zur Beseitigung der Bedrohung

Sie können für Prozesse, die überwacht werden sollen, eine Liste mit benutzerdefinierten Regeln erstellen. Eine neue Regel generieren:

1. Klicken Sie auf die Schaltfläche **+****Hinzufügen** am oberen Ende der Tabelle. Diese Aktion öffnet das Fenster zur Konfiguration einer Regel.
2. Konfigurieren des Moduls unter Verwendung der folgenden Regeleinstellungen:
 - **Name der Regel.** Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll. Für Vorgänge wie `firefox.exe` oder `chrome.exe` beispielsweise, kann die Regel `Browser` heißen.

- **Prozesse.** Geben Sie den Namen der Prozesse ein, die Sie überwachen wollen, und trennen Sie diese durch Semikolon (;).
- **Überwachungsmodus.** Zur Schnellkonfiguration klicken Sie das Sicherheitslevel an, das ihren Bedürfnissen am meisten entspricht (**Aggressiv**, **Normal** or **Tolerant**). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Sie können die Moduleinstellungen detailliert konfigurieren, indem Sie das Schutzlevel **Benutzerdefiniert** anklicken und eine oder mehrere der folgenden Optionen wählen:

- **Hooks werden auf kritische Benutzermodus-DLLs gesetzt.** DLL-Injektionen erkennen, die einen Schad-Code in den aufrufenden Prozess laden.
- **Entpackungs-/Entschlüsselungsversuche in der ausführbaren Hauptdatei.** Erkennt Versuchen, den Code im ausführbaren Hauptprozess zu entschlüsseln und schützt den Prozess vor Veränderung durch bösartige Anweisungen.
- **Fremde Schreibvorgänge im Zielprozess.** Schützt vor Code- Injektion im geschützten Prozess.
- **Exploits.** Erkennt unbeabsichtigtes Prozessverhalten verursacht durch Virus oder Ausnutzung einer vorher nicht bekannten Schwachstelle. Verwenden Sie diese Option, wenn die Code-Ausführung vom Stapel- oder Heap-Speicher der geschützten Anwendung überwacht werden soll.
- **Hooking von WinSock.** Wehrt Ausspionieren von im Betriebssystem verwendeten Netzwerk-Bibliotheken (DLLs) ab und garantiert sichere TCP/IP-Kommunikation.
- **Aktionen.** Es gibt unterschiedliche Aktionen zur Behandlung erkannter Bedrohungen. Jede dieser Aktionen hat wiederum verschiedene Optionen und/oder sekundäre Aktionen. Sie werden im Folgenden beschrieben:

- **Hauptaktion.** Dies ist die direkt anzuwendende Aktion zum Blockieren eines erkannten Angriffs auf die Gastmaschine. Dies sind die verfügbaren Optionen:
 - **Log.** Ereignis in die Datenbank eintragen. In diesem Fall erhalten Sie lediglich eine Benachrichtigung (sofern konfiguriert) und können den Vorfall im **HVI Aktivität**-Bericht anzeigen.
 - **Verweigern.** Weist jeden Versuch der Bedrohung ab, den Zielprozess zu ändern.
 - **Maschine herunterfahren.** Führt die virtuelle Maschine herunter, auf der der Zielprozess läuft.



Wichtig

Es wird empfohlen die Primäraktion zunächst auf **Protokoll** zu setzen. Dann sollte die Richtlinie eine Weile lang verwendet werden, um sicherzugehen, dass alles den Erwartungen entsprechend läuft. Danach können Sie eine beliebige Aktion festlegen, die ausgeführt werden soll, wenn eine Speicherverletzung erkannt wird.

- **Bereinigungsaktion.** Abhängig von der gewählten Option injiziert der Security Server ein Bereinigungs-Tool in das Betriebssystem des Gastes. Das Tool initiiert automatisch einen Malware-Scan und führt die gewählte Aktion aus, wenn eine Bedrohung erkannt wird. Dies sind die verfügbaren Optionen:
 - **Desinfizieren.** Entfernt den Malware-Code aus den infizierten Dateien. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.
 - **Löschen.** Löscht ohne Warnung die erkannte Datei vom Speicher. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
 - **Ignorieren.** Das Bereinigungs-Tool erkennt und meldet die erkannten Dateien.
 - **Keine.** Das Bereinigungs-Tool wird nicht in das Betriebssystem des Gastes injiziert.



Beachten Sie

Das Schließen des Tools entfernt es auch aus dem System; es hinterlässt keine Spuren im Gast-Betriebssystem.


- **Ersatzaktion zur Bereinigung.** Falls die Bereinigungsaktion nicht greift, kann eine andere Bereinigungsverfahren aus den Optionen gewählt werden.

3. Klicken Sie auf **Speichern**.

Nach Erstellung können Regeln jederzeit bearbeitet werden. Durch Anklicken der Regelbezeichnung öffnet sich das Regelkonfigurations-Fenster.

GravityZone ermöglicht zudem durch gleichzeitige Änderung mehrerer Regeln die schnelle Konfiguration des Memory-Introspection-Verhaltens bei Funden. Mehrere Regeln mit den gleichen Aktionen einstellen:

1. Regeln auswählen, die geändert werden sollen.
2. **Aktion und Bereinigung** oben in der Tabelle anklicken.
3. Die für jede Aktion gewünschte Option auswählen.
4. Klicken Sie auf **Speichern**. Neue Aktionen werden wirksam, sobald die Richtlinie gespeichert wird, vorausgesetzt die entsprechende Maschine ist online.

Um eine oder mehrere Regeln aus der Liste zu entfernen, wählen Sie diese aus und klicken Sie  **Löschen** oben in der Tabelle an.

Forensische Informationen

Markieren Sie das Kästchen **Anwendungsabsturz-Ereignisse** unter der Tabelle der Benutzerbereichs-Regeln, wenn Sie bei Anwendungsabbrüchen detaillierte Informationen sammeln möchten.

Sie können diese Informationen im HVI-Aktivitätsbericht einsehen und den Grund herausfinden, weshalb die Anwendung abgebrochen wurde. Wenn das Ereignis im Zusammenhang mit einem Angriff steht, werden die entsprechenden Details zusammen mit anderen Ereignissen unter dem entsprechenden Vorfall gruppiert, der das Ereignis verursachte.

Kernel-Bereich

HVI schützt die wichtigsten Elemente des Betriebssystems, wie z.B.:

- Kritische Kernel-Treiber und verbundene Treiberobjekte mit schnellen I/O-Verzweigungstabellen und verbundene Core-Treiber.

- Netzwerktreiber, deren Änderung es einer Malware ermöglichen würde, den Datenverkehr zu unterbrechen und bösartige Komponenten in den Verkehrsstrom zu injizieren.
- Kernel-Image des Betriebssystems mit den folgenden Elementen: Code-Bereich, Daten-Bereich und schreibgeschützter Bereich einschließlich Import Address Table (IAT), Export Address Table (EAT) und Ressourcen.

In diesem Bereich können Sie die Sicherheitseinstellungen für Prozesse im Kernel-Bereich-Speicher konfigurieren.

Verwenden Sie das Kontrollfeld **Memory Introspection Kernel-Bereich** zur Aktivierung oder Deaktivierung des Schutzes.

Zur Schnellkonfiguration klicken Sie das Sicherheitslevel an, das Ihren Bedürfnissen am meisten entspricht (**Aggressiv**, **Normal** oder **Tolerant**). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Sie können die Moduleinstellungen detailliert konfigurieren, indem Sie das Schutzlevel **Benutzerdefiniert** anklicken und eine oder mehrere der folgenden Optionen wählen:

- **Steuerungsregister.** Steuerregister (CR) sind Prozessorregister zur Steuerung des generellen Verhaltens eines Prozessors oder eines anderen digitalen Geräts. Wählen Sie diese Option, um Ladeversuche ungültiger Werte in bestimmte Steuerregister zu erkennen.
- **Model Specific Registers.** Diese Register beziehen sich auf jedes der verschiedenen Steuerregister im x86-Befehlssatz zum Debugging, zur Programmausführungs- und Rechnerleistungsüberwachung und zum Umschalten bestimmter CPU-Funktionen. Wählen Sie diese Option, um Änderungsversuche an diesen Register zu entdecken.
- **IDT/GDT-Integrität.** Global oder Interrupt Descriptor Tables (IDT/GDT) werden vom Prozessor verwendet, um die geeignete Reaktion auf Unterbrechungen oder Ausnahmen festzulegen. Wählen Sie diese Option, um Änderungsversuche an diesen Tabellen zu erkennen.
- **Anti-Malware-Treiberschutz.** Wählen Sie diese Option, um Änderungsversuche an Treibern zu erkennen, die von der Malware-Schutz-Software verwendet werden.
- **Xen-Treiberschutz.** Wählen Sie diese Option, um Änderungsversuche an Treibern des Citrix XenServer-Hypervisor zu erkennen.

Es gibt es mehrere mögliche Aktionen zum Umgang mit erkannten Bedrohungen. Jede dieser Aktionen hat wiederum verschiedene Optionen und/oder sekundäre Aktionen. Sie werden im Folgenden beschrieben:

- **Hauptaktion.**

- **Log.** Ereignis in die Datenbank eintragen. In diesem Fall erhalten Sie lediglich eine Benachrichtigung (sofern konfiguriert); der Vorfall kann im Bericht **Memory Introspection Aktivität** angezeigt werden.
- **Verweigern.** Weist jeden Versuch der Bedrohung ab, den Zielprozess zu ändern.
- **Maschine herunterfahren.** Fährt die virtuelle Maschine herunter, auf der der Zielprozess läuft.



Wichtig

Es wird empfohlen die Primäraktion zunächst auf **Protokoll** zu setzen. Dann sollte die Richtlinie eine Weile lang verwendet werden, um sicherzugehen, dass alles den Erwartungen entsprechend läuft. Danach können Sie eine beliebige Aktion festlegen, die ausgeführt werden soll, wenn eine Speicherletzung erkannt wird.

- **Bereinigungsaktion.**

- **Desinfizieren.** Entfernt den Malware-Code aus den infizierten Dateien. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.
- **Löschen.** Löscht ohne Warnung die erkannte Datei vom Speicher. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Ignorieren.** Das Bereinigungs-Tool erkennt und meldet die erkannten Dateien.
- **Keine.** Das Bereinigungs-Tool wird nicht in das Betriebssystem des Gastes injiziert.

- **Ersatzaktion zur Bereinigung.** Falls die Bereinigungsaktion nicht greift, kann eine andere Bereinigungsverfahren aus den Optionen gewählt werden.

Darüber hinaus können Sie wahlweise Informationen sammeln, die die Daten ergänzen, die forensischen Teams zur Verfügung gestellt werden. Markieren Sie die Kästchen **Betriebssystemfehlerereignisse** und **Treiberereignisse**, um zu ermöglichen, dass Informationen zu Gastbetriebssystemfehlern oder zu Ereignissen gesammelt werden, die durch vom Betriebssystem geladenen zusätzlichen Modulen

generiert werden. Diese Ereignisse im Vorfeld eines Vorfalls können die forensische Suche nach der Ursache des Angriffs beschleunigen.

Diese Ereignisse werden im HVI-Aktivitätsbericht unter dem Vorfall aggregiert, der sie verursacht hat.

Ausschlüsse

Mit GravityZone können Sie Prozesse von den HVI-Scans unter Verwendung der Berichte **Blockierte Anwendungen** and **HVI-Aktivität** ausschließen. Im Bereich **Ausschlüsse** werden diese Prozesse aus den genannten Berichten gesammelt und in Form einer einer Tabelle angezeigt.

Sie können für jeden ausgeschlossenen Prozess einen Kommentar mit dem Ausschlussgrund anzeigen.

Sollten Sie sich hinsichtlich eines ausgeschlossenen Prozesses umentscheiden, klicken Sie oben in der Tabelle auf **Löschen**, um den Prozess in zukünftigen Scans wieder zu berücksichtigen.

Benutzerdefinierte Tools

In diesem Bereich können Sie die Toolinjektion in den Ziel-Gastbetriebssystemen konfigurieren. Um diese Tools nutzen zu können, müssen sie zunächst in GravityZone hochgeladen werden. Weitere Informationen finden Sie unter [„Benutzerdefiniert Tool-Injektion mit HVI“ \(S. 511\)](#).

Gehen Sie zur Konfiguration der Injektionen folgendermaßen vor:

1. Aktivieren oder deaktivieren Sie die Funktion über das Kästchen **Injektionen aktivieren**.
2. Klicken Sie oben in der Tabelle auf die **+ Hinzufügen**-Schaltfläche, um ein neues Tool hinzuzufügen. Ein Konfigurationsfenster wird geöffnet.
3. Wählen Sie das entsprechende Tool aus der **Tool auswählen**-Dropdown-Liste. Diese Tools wurden zuvor in GravityZone hochgeladen. Wenn das gesuchte Tool in der Liste nicht aufgeführt ist, rufen Sie das **Tool-Verwaltungszentrum** auf und fügen Sie es von dort aus hinzu. Weitere Informationen finden Sie unter [„Benutzerdefiniert Tool-Injektion mit HVI“ \(S. 511\)](#).
4. Geben Sie unter **Tool-Beschreibung** den Verwendungszweck des Tools und ggf. weitere Informationen ein, die Sie als hilfreich erachten.

5. Geben Sie die Befehlszeile des Tools gemeinsam mit allen benötigten Eingabeparametern ein, so wie Sie es auch in der Eingabeaufforderung bzw. im Terminal tun würden. Zum Beispiel:

```
bash script.sh <param1> <param2>
```

Für die BD-Bereinigungstools können Sie aus den beiden Klappmenüs nur die Bereinigungsaktion sowie die Ersatzaktion zur Bereinigung auswählen.

6. Verweisen Sie auf den Speicherort, von dem der Security Server die Protokolle abrufen soll:

- **stdout**. Markieren Sie das Kästchen, um die Protokolle über den Standard-Ausgangsübertragungskanal abzurufen.
- **Ausgabedatei**. Markieren Sie dieses Kästchen, um auf dem Endpunkt gespeicherte Protokolldateien abzurufen. In diesem Fall müssen Sie den Pfad eingeben, über den der Security Server die Datei finden kann. Sie können sowohl absolute Pfade als auch Systemvariablen eingeben.

Ihnen stehen hier zudem zwei weitere Optionen zur Auswahl:

- a. **Protokolldateien nach der Übermittlung vom Gast löschen**. Wählen Sie diese Option, wenn die Dateien auf dem Endpunkt nicht mehr benötigt werden.
 - b. **Protokolle übermitteln an**. Wählen Sie diese Option, um die Protokolldateien vom Security Server zu einem anderen Speicherort zu verschieben. Zu diesem Zwecke müssen Sie den Pfad zum Zielspeicherort und die Anmeldeinformationen für die Authentifizierung angeben.
7. Legen Sie fest, wie die Injektion ausgelöst werden soll. Sie haben die folgenden Möglichkeiten:
- **Nachdem auf einer Gast-VM eine Verletzung gefunden wurde**. Das Tool wird sofort nach Erkennung einer Bedrohung auf der virtuellen Maschine injiziert.
 - **Nach einem festgelegten Plan**. Verwenden Sie die Planungsoptionen, um einen Zeitplan für die Injektion zu konfigurieren. Sie können festlegen, dass das Tool alle paar Stunden, Tage oder Wochen ausgeführt wird und Datum und Zeitpunkt der ersten Ausführung bestimmen.

Bitte beachten Sie, dass die virtuelle Maschine zum geplanten Zeitpunkt eingeschaltet sein muss. Eine geplante Injektion wird nicht ausgeführt, wenn die Maschine ausgeschaltet oder pausiert ist. Es empfiehlt sich für solche Fälle das Kästchen **Wenn die geplante Injektionszeit verpasst wurde, Aufgabe sobald wie möglich ausführen** zu aktivieren.

- Gelegentlich braucht das Tool unter Umständen länger als erwartet, um den Auftrag abzuschließen, oder reagiert nicht mehr. Um in diesen Fällen Abstürze zu verhindern, können Sie im Bereich **Sicherheitskonfiguration** festlegen, nach wie vielen Stunden der Security Server den Tool-Prozess automatisch beenden soll.
- Klicken Sie auf **Speichern**. Das Tool wird in der Tabelle hinzugefügt.

Gehen Sie wie eben beschrieben vor, um weitere, beliebig viele Tools hinzuzufügen.

7.2.3. Malware-Schutz



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server
- Linux
- macOS

Das Modul für den Malware-Schutz schützt Sie vor allen Arten von Bedrohungen durch Malware (Viren, Trojaner, Spyware, Rootkits, Adware usw.). Der Schutz wird in drei Kategorien unterteilt:

- Zugriff-Scans: Verhindern, dass neue Malware-Bedrohungen auf das System gelangen.
- Scan bei der Ausführung: proaktiver Schutz vor Bedrohungen.
- Bedarf-Scans: Malware, die sich bereits im System befindet, kann entdeckt und entfernt werden.

Wenn der Bitdefender-Sicherheitsagent einen Virus oder andere Malware findet, versucht das Programm automatisch, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infektion zu isolieren. In der Quarantäne kann

ein Virus keinen Schaden anrichten, denn er kann weder ausgeführt noch geöffnet werden.

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden.

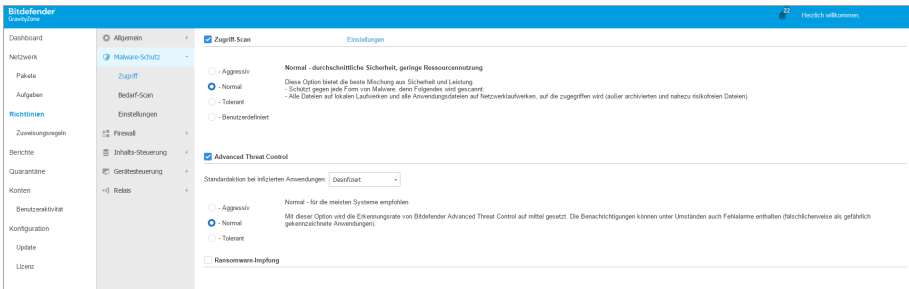
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Zugriff
- Bei Ausführung
- Bedarf-Scan
- HyperDetect
- Erweiterter Exploit-Schutz
- Einstellungen
- Security Server

Zugriff

In diesem Abschnitt können Sie die Komponenten konfigurieren, die den Schutz bei Zugriffen auf Dateien oder Anwendungen gewährleisten:

- Zugriff-Scan
- Ransomware-Impfung



Richtlinien - Zugriff-Scan-Einstellungen

Zugriff-Scan

Zugriff-Scans verhindern, dass neue Malware auf das System gelangt, indem lokale und Netzwerk-Dateien gescannt werden, sobald auf sie zugegriffen wird (öffnen, verschieben, kopieren oder ausführen). Ferner werden Boot-Sektoren und potenziell unerwünschte Anwendungen (PUA) gescannt.

**Beachten Sie**

Diese Funktion unterliegt auf Linux-Systemen gewissen Einschränkungen. Weitere Einzelheiten finden Sie im Anforderungskapitel im GravityZone-Installationshandbuch.

Um die Zugriffs-Scans zu konfigurieren:

1. Über das Kästchen können Sie Zugriffs-Scans aktivieren oder deaktivieren.

**Warnung**

Wenn Sie Zugriff-Scans deaktivieren, werden die Endpunkte anfällig für Malware.

2. Zur Schnellkonfiguration klicken Sie die Sicherheitsstufe an, die Ihren Bedürfnissen am besten entspricht (aggressiv, normal, tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.
3. Sie können Details der Scan-Einstellungen konfigurieren, indem Sie die Sicherheitsstufe **Benutzerdefiniert** wählen und auf den Link **Einstellungen** klicken. Das Fenster für die **Zugriff-Scan-Einstellungen** wird angezeigt. Hier finden Sie unter den Reitern **Allgemein** und **Erweitert** eine Reihe von Optionen.

Die Optionen im Reiter **Allgemein** werden im Folgenden beschrieben:

- **Datei-Speicherort.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Die Scan-Einstellungen für lokale Dateien (auf dem lokalen Endpoint gespeichert) und Netzwerkdateien (auf den Netzwerklaufwerken gespeichert) können separat festgelegt werden. Wenn der Malware-Schutz auf allen Computern im Netzwerk installiert ist, ist es möglich, den Scan der Netzwerkdateien zu deaktivieren, um den Netzwerkzugriff zu beschleunigen.

Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle aufgerufenen Dateien (unabhängig von der Dateierdung), oder nur für Anwendungsdateien oder nur für bestimmte Dateierdungen, die Sie für gefährlich erachten, durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

**Beachten Sie**

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter [„Anwendungsdateitypen“ \(S. 545\)](#).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf **Speichern**.



Beachten Sie

Auf Linux-Systemen wird bei Dateierweiterungen zwischen Groß- und Kleinschreibung unterschieden, wodurch Dateien mit dem gleichen Namen und unterschiedlichen Erweiterungen wie separate Objekte behandelt werden. So unterscheidet sich z. B. `file.txt` von `file.TXT`.

Sie können auch große Dateien vom Scan ausschließen, um die Systemleistung nicht zu stark zu beeinträchtigen. Markieren Sie das Kästchen **Maximale Größe (MB)** geben Sie die Größe an, bis zu der Dateien gescannt werden sollen. Gehen Sie mit dieser Einstellung vorsichtig um, denn Malware kann auch größere Dateien befallen.

- **Scan.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
 - **Nur neue oder geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
 - **Boot-Sektoren.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Code um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
 - **Für Keylogger.** Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
 - **Für potenziell unerwünschte Anwendungen (PUA).** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen,

unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

- **Archive.** Wählen Sie diese Option, wenn Sie Zugriff-Scans für archivierte Dateien aktivieren möchten. Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und bei deaktivierten Zugriff-Scans ausgeführt wird.

Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:

- **Maximale Archivgröße (MB).** Sie können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
- **Maximale Archvertiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archvertiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.
- **Verzögerte Scans.** Verzögerte Scans verbessern die Systemleistung bei der Durchführung von Dateizugriffsvorgängen. So werden zum Beispiel Systemressourcen durch das Kopieren großer Dateien nicht beeinträchtigt. Die Option ist standardmäßig aktiviert.
- **Prüfaktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
 - **Standardaktion für infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI). Der Bitdefender-Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

Wenn eine infizierte Datei gefunden wird, versucht der Bitdefender-Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen. Sie können diesen empfohlenen Ablauf nach Ihren Bedürfnissen abändern.

**Wichtig**

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Standardaktion für verdächtige Dateien.** Dateien werden durch heuristische Analysen und andere Bitdefender-Technologien als verdächtig erkannt. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden). Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Wenn eine verdächtige Datei gefunden wird, wird den Benutzern der Zugriff auf diese Datei verwehrt, um eine potenzielle Infektion zu verhindern.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können für jeden Dateityp zwei Aktionen festlegen. Folgende Aktionen stehen zur Verfügung:

Zugriff verweigern

Zugriff auf infizierte Dateien verweigern.

**Wichtig**

Bei Mac-Endpunkten wird statt der Aktion **Zugriff verweigern** die Aktion **In die Quarantäne verschieben** ausgeführt.

Desinfizieren

Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen

Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Dateien in Quarantäne verschieben

Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.

Sie können die Dateien in Quarantäne über die [Quarantäne](#)-Seite in der Konsole verwalten.

Keine Aktion ausführen



Nur die infizierten Dateien melden, die von Bitdefender gefunden wurden.

Im Reiter **Erweitert** geht es um Zugriff-Scans für Linux-Maschinen. Über das Kästchen können Sie die Funktion aktivieren und deaktivieren.

In der unten stehenden Tabelle können Sie die Linux-Verzeichnisse festlegen, die Sie scannen möchten. Standardmäßig gibt es hier fünf Einträge für jeweils bestimmte Speicherorte auf den Endpunkten: `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

So fügen Sie weitere Einträge hinzu:

- Geben Sie einen beliebigen Speicherort in das Suchfeld oben in der Tabelle ein.
- Wählen Sie die vordefinierten Verzeichnisse aus der Liste, die angezeigt wird, wenn Sie auf den Pfeil am rechten Rand des Suchfelds klicken.

Klicken Sie auf die Schaltfläche  **Hinzufügen**, um einen Speicherort in der Tabelle zu speichern, und  **Löschen**, um einen Speicherort aus der Liste zu entfernen.

Ransomware-Impfung

Die Ransomware-Impfung immunisiert Ihre Computer gegen **bereits bekannte** Ransomware und verhindert so den Verschlüsselungsvorgang, auch wenn die Infektion bereits erfolgt ist. Über dieses Kästchen können Sie Ihre Ransomware-Impfung aktivieren oder deaktivieren.

Die Funktion Ransomware-Impfung ist standardmäßig deaktiviert. Die Bitdefender Labs untersuchen das Verhalten weit verbreiteter Ransomware-Varianten. Mit jedem Update der Sicherheitsinhalte werden neue Signaturen bereitgestellt, um auch neueste Bedrohungen zu neutralisieren.



Warnung

Um noch besseren Schutz vor Ransomware-Infektionen zu gewährleisten, sollten Sie Vorsicht im Umgang mit unerwünschten und verdächtigen Anhängen walten lassen und sicherstellen, dass die Sicherheitsinhalte regelmäßig aktualisiert werden.



Beachten Sie

Ransomware-Impfung ist nur mit Bitdefender Endpoint Security Tools für Windows verfügbar.

Bei Ausführung

In diesem Abschnitt können Sie den Schutz konfigurieren, der bei der Ausführung von schädlichen Prozessen greift: Dies gilt für die folgenden Schutzebenen:

Advanced Threat Control

i **Beachten Sie**
Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server
- macOS

Advanced Threat Control von Bitdefender ist eine Technologie zu vorbeugenden Erkennung, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

Advanced Threat Control überwacht kontinuierlich die auf Ihrem Endpunkt laufenden Anwendungen auf Malware-ähnliche Aktionen. Jede einzelne dieser Aktionen erhält einen Wert, und jeder Prozess erhält so einen aggregierten Gesamtwert. Wenn diese Gesamteinstufung eine bestimmte Schwelle überschreitet, wird der entsprechende Prozess als schädlich eingestuft.

Advanced Threat Control wird automatisch versuchen, die gefundene Datei zu desinfizieren. Wenn die Desinfektionsroutine fehlschlägt, löscht Advanced Threat Control die Datei.

i **Beachten Sie**
Bevor die Desinfektion durchgeführt wird, wird eine Kopie der Datei in der Quarantäne abgelegt, damit Sie die Datei bei Bedarf später wiederherstellen können. Diese Aktion kann im Reiter **Malware-Schutz > Einstellungen** der Richtlinieneinstellungen mit der Option **Dateien vor der Desinfektion in die Quarantäne kopieren** konfiguriert werden. Diese Option ist in den Richtlinienvorlagen standardmäßig aktiviert.

So konfigurieren Sie die Advanced Threat Control:

1. Über das Kästchen können Sie Advanced Threat Control aktivieren oder deaktivieren.

✘ **Warnung**
Wenn Sie Advanced Threat Control deaktivieren, werden die Computer anfällig für unbekannte Malware.

2. Die Standardaktion für infizierte Anwendungen, die von Advanced Threat Control gefunden werden, ist Desinfektion. Über das Menü kann eine andere Standardaktion gewählt werden.
 - Mit **Blockieren** verwehren Sie einer infizierten Anwendung den Zugriff.
 - Wählen Sie **Keine Aktion ausführen**, wenn Sie lediglich eine von Bitdefender erkannte infizierte Applikation melden wollen.
3. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (**aggressiv, normal oder tolerant**). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.



Beachten Sie

Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Advanced Threat Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen, aber auch die Wahrscheinlichkeit von Fehlalarmen (ungefährlichen Anwendungen, die dennoch als schädlich eingestuft wurden).

Es wird dringend empfohlen, Ausschlussregeln für häufig genutzte oder bekannte Anwendungen zu erstellen, um Fehlalarme zu vermeiden (ungefährliche Anwendungen, die fälschlicherweise erkannt werden). Klicken Sie auf den Reiter [Malware-Schutz](#) > [Einstellungen](#) und konfigurieren Sie die ATC/IDS-Prozessausschlussregeln für vertrauenswürdige Anwendungen.



Richtlinien für Computer und virtuelle Maschinen - ATC/IDS-Prozessausschluss

Ransomware-Abhilfemaßnahme

Ransomware-Abhilfemaßnahme verwendet Erkennungs- und Bereinigungstechnologien, um Ihre Daten vor Ransomware-Angriffen zu schützen. Unabhängig davon, ob die Ransomware bereits bekannt oder neu ist, erkennt GravityZone anormale Verschlüsselungsversuche und blockiert den Prozess.

Danach stellt es die Dateien von Sicherungskopien an ihrem ursprünglichen Speicherort wieder her.



Wichtig

Für die Ransomware-Abhilfemaßnahmen wird die Active Threat Control benötigt.



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

So können Sie die Ransomware-Abhilfemaßnahmen konfigurieren:

1. Markieren Sie das Kästchen **Ransomware-Abhilfemaßnahme** im Richtlinienabschnitt **Malware-Schutz > Bei Ausführung**, um die Funktion zu aktivieren.
2. Wählen Sie die Überwachungsmodi aus, die Sie verwenden möchten:
 - **Lokal.** GravityZone überwacht die Prozesse und erkennt lokal auf dem Endpunkt gestartete Ransomware-Angriffe. Diese Option wird für Arbeitsplatzrechner empfohlen und ist auf Servern wegen der Leistungsbeeinträchtigung nur mit Vorsicht zu verwenden.
 - **Remote.** GravityZone überwacht den Zugriff auf Netzwerkfreigabepfade und erkennt Ransomware-Angriffe, die von einem anderen Rechner aus gestartet werden. Verwenden Sie diese Option, wenn der Endpunkt ein Dateiserver ist oder dort Netzwerkfreigaben aktiviert sind.
3. Wählen Sie die Wiederherstellungsmethode aus:
 - **Bei Bedarf.** Sie wählen manuell die Angriffe aus, für die die Dateien wiederhergestellt werden sollen. Sie können dies auf der Seite **Berichte > Ransomware-Aktivität** aus jederzeit nach Belieben tun, jedoch nicht später als 30 Tage nach dem Angriff. Danach ist ein Wiederherstellung nicht mehr möglich.
 - **Automatisch.** GravityZone stellt die Dateien unmittelbar nach einer Ransomware-Erkennung automatisch wieder her.

Damit die Wiederherstellung erfolgreich durchgeführt werden kann, müssen Endpunkte verfügbar sein.

Nach der Aktivierung haben Sie mehrere Optionen, um zu prüfen, ob Ihr Netzwerk einem Ransomware-Angriff ausgesetzt ist:

- Rufen Sie Ihre Benachrichtigungen auf und suchen Sie nach **Ransomware-Fund**. Weitere Informationen zu dieser Benachrichtigung finden Sie unter „[Benachrichtigungsarten](#)“ (S. 513).
- Rufen Sie den Bericht **Sicherheitsüberprüfung** auf.
- Rufen Sie die Seite **Ransomware-Aktivität** auf.

Weiter unten auf dieser Seite können Sie bei Bedarf Wiederherstellungsaufgaben starten. Weitere Informationen finden Sie unter [???](#).

Falls Sie einen Fund bemerken, bei dem es sich um einen harmlosen Verschlüsselungsprozess handelt, falls Sie Dateiverschlüsselung für bestimmte Pfade erlauben oder falls Sie den Fernzugriff von bestimmten Rechnern aus erlauben, fügen Sie diese Ausschlüsse im Richtlinienabschnitt **Malware-Schutz > Einstellungen > Benutzerdefinierte Ausschlüsse** hinzu. Die Ransomware-Abhilfemaßnahmen erlauben Ausschlüsse für Ordner, Prozesse und IP/Maske. Weitere Informationen finden Sie unter „[Ausschlüsse](#)“ (S. 301).

Bedarf-Scan

In diesem Bereich können Sie Malware-Scan-Aufgaben hinzufügen und konfigurieren, die dann regelmäßig nach einem definierten Zeitplan auf den gewünschten Computern ausgeführt werden.

<input type="checkbox"/>	Aufgabenname	Aufgabentyp	Wiederholungsintervall	Erste Ausführung
<input type="checkbox"/>	Meine Aufgabe	Quick Scan	1 Woche(n)	10/07/2015 11:51

Geräte-Scan ⓘ

- CD-/DVD-Datenträger
- USB-Speichergeräte
- Zugeordnete Netzlaufwerke
- Keine Geräte scannen, die mehr Daten gespeichert haben als (MB)

Richtlinien für Computer und virtuelle Maschinen - Bedarf-Scan-Aufgaben

Der Scan erfolgt unauffällig im Hintergrund, unabhängig davon, ob der Benutzer am System angemeldet ist oder nicht.

Obwohl nicht zwingend erforderlich, empfiehlt es sich, einen umfassenden System-Scan einzuplanen, der wöchentlich auf allen Endpunkten ausgeführt wird. Regelmäßige Scans der Endpunkte bieten vorbeugende Sicherheit. Nur so können Malware-Bedrohungen erkannt und blockiert werden, die den Echtzeitschutz unter Umständen umgehen haben.

Neben den regelmäßigen Scans können Sie auch eine [automatische Erkennung und Prüfung](#) von externen Speichermedien konfigurieren.

Scan-Aufgaben verwalten

Die Scan-Aufgaben-Tabelle informiert Sie über bestehende Scan-Aufgaben und enthält wichtige Informationen zu den einzelnen Aufgaben:

- Name und Art der Aufgabe.
- Zeitplan, anhand dessen die Aufgabe regelmäßig ausgeführt wird (Wiederholung).
- Zeitpunkt, zu dem die Aufgabe das erste Mal ausgeführt wurde.

Sie können die folgenden Typen von Scan-Aufgaben hinzufügen und konfigurieren:

- **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenskan in Anspruch nehmen würde.

Wenn Malware oder Rootkits gefunden werden, desinfiziert Bitdefender sie automatisch. Wenn die Datei aus irgendeinem Grund nicht desinfiziert werden kann, wird sie in die Quarantäne verschoben. Dieser Art Scan ignoriert verdächtige Dateien.

Der Quick-Scan ist eine Standard-Scan-Aufgabe mit vorkonfigurierten Optionen, die nicht geändert werden können. Pro Richtlinie können Sie nur eine Quick-Scan-Aufgabe hinzufügen.

- Der **Vollständige Scan** durchsucht den gesamten Endpunkt nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, z. B. Viren, Spyware, Adware, Rootkits usw.

Bitdefender versucht automatisch als infiziert erkannte Dateien zu desinfizieren. Sollte die Malware nicht entfernt werden können, wird sie in die Quarantäne verschoben, wo sie keinen Schaden mehr anrichten kann. Verdächtige Dateien werden ignoriert. Wenn Sie auch für verdächtige Dateien Aktionen ausführen möchten oder für infizierte Dateien andere Standardaktionen definieren möchten, führen Sie einen benutzerdefinierten Scan durch.

Der Vollständige Scan ist eine Standard-Scan-Aufgabe mit vorkonfigurierten Optionen, die nicht geändert werden können. Pro Richtlinie können Sie nur eine Vollständiger-Scan-Aufgabe hinzufügen.

- Bei einem **benutzerdefinierten Scan** können Sie die Orte, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.
- **Netzwerk-Scan** ist ein benutzerdefinierten Scan, bei dem Sie zunächst einen einzelnen verwalteten Endpunkt bestimmen, über den Netzwerklaufwerke gescannt werden, und dann die Scan-Optionen und die zu scannenden Speicherorte konfigurieren können. Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.

Die wiederkehrende Netzwerk-Scan-Aufgabe wird nur an den ausgewählten Scanner-Endpunkt gesendet. Wenn der entsprechende Endpunkt nicht verfügbar ist, werden die Einstellungen für lokalen Scan angewendet.

**Beachten Sie**

Netzwerk-Scan-Aufgaben können Sie nur innerhalb einer Richtlinie erstellen, die bereits einem Endpunkt zugewiesen ist, der als Scanner verwendet werden kann.

Neben den Standard-Scan-Aufgaben (die Sie nicht löschen oder kopieren können) können Sie beliebig viele benutzerdefinierte (Netzwerk-)Scan-Aufgaben erstellen.

Um eine neue benutzerdefinierte (Netzwerk-)Scan-Aufgabe zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle. Um die Einstellungen für eine bestehende Scan-Aufgabe zu ändern, klicken Sie auf den Namen der entsprechenden Aufgabe. Bitte rufen Sie das folgende Thema auf, um mehr über die Konfiguration der Aufgabeneinstellungen zu erfahren.

Um eine Aufgabe aus der Liste zu entfernen, klicken Sie auf die Schaltfläche **- Löschen** auf der rechten Seite der Tabelle.

Konfiguration einer Prüfaufgabe

Die Einstellungen für die Scan-Aufgaben sind auf drei Reiter verteilt:

- **Allgemein:** Aufgabenname und Zeitplanung festlegen.
- **Optionen:** Scan-Profil für eine schnelle Konfiguration der Scan-Einstellungen auswählen und Einstellungen für benutzerdefinierte Scans festlegen.
- **Ziel:** Hier können Sie die Dateien und Ordner auswählen, die gescannt werden sollen, und solche definieren, die vom Scan ausgeschlossen werden sollen.

Im Folgenden werden die Optionen vom ersten bis zum letzten Reiter beschrieben:

Aufgabe bearbeiten

Allgemein Optionen Ziel

Details

Aufgabenname:

Aufgabe mit niedriger Priorität ausführen

Computer nach Abschluss des Scans herunterfahren

Planner

Startdatum und -zeit: 09/22/2016 11:15

Wiederholung

Regelmäßige Ausführung der Aufgabe planen: einmal alle: 1 Tag(e)

Ausführung der Aufgabe jeden: So Mo Di Mi Do Fr Sa

Wenn die geplante Ausführungszeit verpasst wurde, Aufgabe sobald wie möglich ausführen

Überspringen, wenn es bis zum Start des nächsten geplanten Scans nur noch weniger sind als 1 Tag(e)

Speichern Abbrechen

Richtlinien für Computer und virtuelle Maschinen - Konfiguration der allgemeinen Einstellungen für Bedarf-Scan-Aufgaben

- **Details.** Geben Sie der Aufgabe einen eindeutigen Namen, der ihren Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie das Ziel der Scan-Aufgabe und unter Umständen auch die Scan-Einstellungen.

Scan-Aufgaben werden standardmäßig mit niedrigerer Priorität ausgeführt. So stellt Bitdefender sicher, dass andere Programme schneller laufen können; der Scan dauert aber länger. Über das Kästchen **Aufgabe mit niedriger Priorität ausführen** können Sie diese Funktion deaktivieren und wieder aktivieren.



Beachten Sie

Diese Option gilt nur für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent).

Können Sie das Kästchen **Computer nach Abschluss des Scans herunterfahren** wählen, um den Computer auszuschalten, falls Sie ihn länger nicht benutzen wollen.



Beachten Sie

Diese Option gilt für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent) und Endpoint Security for Mac.

- **Planer.** Verwenden Sie die Planungsoptionen, um den Scan-Zeitplan zu konfigurieren. Sie können festlegen, dass der Scan alle paar Stunden, Tage oder Wochen durchgeführt wird und Datum und Zeit des ersten Scans bestimmen.

Zum definierten Zeitpunkt müssen die Endpunkte eingeschaltet sein. Eine geplante Scan-Aufgabe kann nicht ausgeführt werden, wenn die Maschine zu diesem Zeitpunkt nicht eingeschaltet ist, sich im Ruhezustand oder im Energiesparmodus befindet. In diesen Fällen wird der Scan bis zum nächsten Mal verschoben.



Beachten Sie

Der geplante Scan wird zur lokalen Zeit des Zielpunkts ausgeführt. Wenn der geplante Scan zum Beispiel um 18:00 starten soll und der Endpunkt in einer anderen Zeitzone als das Control Center ist, wird der Scan um 18:00 Uhr (Endpunkt-Zeit) gestartet.

Sie können optional festlegen, was passieren soll, wenn die Scan-Aufgabe nicht zur geplanten Zeit gestartet werden konnte (weil der Endpunkt offline oder ausgeschaltet war). Nutzen Sie bei Bedarf die Option **Wenn die geplante Ausführungszeit verpasst wird, Aufgabe so bald wie möglich ausführen**:

- Wenn Sie diese Option unmarkiert lassen, wird zum nächsten geplanten Zeitpunkt versucht, die Scan-Aufgabe zu starten.
 - Wenn Sie die Option markieren, erzwingen Sie, dass der Scan so bald wie möglich durchgeführt wird. Um den besten Zeitpunkt für den Scan zu finden und Benutzer während ihrer Arbeit nicht zu stören, wählen Sie **Überspringen, wenn es bis zum Start des nächsten geplanten Scans nur noch weniger sind als**, und legen Sie den gewünschten Zeitraum fest.
- **Scan-Optionen.** Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren. Markieren Sie dazu das Kästchen **Benutzerdefiniert** und gehen Sie dann zum Bereich **Einstellungen**.

Scan-Aufgabe

Allgemein Optionen Ziel

Prüfoptionen

- Aggressiv Benutzerdefiniert - vom Administrator festgelegte Einstellungen

- Normal

- Tolerant

- Benutzerdefiniert

› Einstellungen

Speichern Abbrechen

Computer-Scan-Aufgabe - Konfiguration eines benutzerdefinierten Scans

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateierdung), oder nur für Anwendungsdateien oder nur für bestimmte Dateierdungen, die Sie für gefährlich erachten, durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.



Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „[Anwendungsdateitypen](#)“ (S. 545).

Wenn Sie nur bestimmte Dateierdungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf **Speichern**.

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierte Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen,

um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.



Beachten Sie

Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten. Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
 - **Archivgröße begrenzen auf (MB).** Sie können Sie die maximale Größe der Archive angeben, die gescannt werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
 - **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.
- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.



Beachten Sie

Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
 - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Code um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
 - **Registrierung scannen.** Wählen Sie diese Option, um die Registrierungsschlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die

Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.

- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach **Rootkits** und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, um nach **Keylogger**-Software zu suchen.
- **Netzwerkfreigaben scannen.** Mit dieser Option werden bereitgestellte Netzwerklaufwerke überprüft.

Für Schnell-Scans ist diese Option standardmäßig deaktiviert. Für vollständige Scans ist diese Option standardmäßig aktiviert. Bei benutzerdefinierte Scans ist die Option **Netzwerkfreigaben scannen** automatisch aktiviert, wenn Sie als Sicherheitsstufe **aggressiv/normal** wählen. Falls Sie die Sicherheitsstufe **tolerant** wählen, wird die Option **Netzwerkfreigabe scannen** automatisch deaktiviert.

- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Browsern auf dem Endpunkt gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Auf potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.
- **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
 - **Standardaktion für infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen,

darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI). Der -Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

Wenn eine infizierte Datei gefunden wird, versucht der -Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.



Wichtig

Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Standardaktion für verdächtige Dateien.** Dateien werden durch heuristische Analysen und andere Bitdefender-Technologien als verdächtig erkannt. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden). Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden. Dateien in Quarantäne werden zu Analyse Zwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Standardaktion für Rootkits.** Rootkits sind spezielle Software-Werkzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie. Wählen Sie aus den entsprechenden Menüs die erste und zweite Aktion, die für

jeden entdeckten Dateityp vorgenommen werden soll. Folgende Aktionen stehen zur Verfügung:

Keine Aktion ausführen

Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

Desinfizieren

Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen

Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Dateien in Quarantäne verschieben

Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die [Quarantäne](#)-Seite in der Konsole verwalten.


- **Scan-Ziel.** Fügen Sie der Liste alle Pfade hinzu, die auf den Ziel-Computern gescannt werden sollen.

Um eine neue Datei oder einen neuen Ordner zum Scan hinzuzufügen:

1. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scannen lassen möchten.
2. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.
 - Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen. Um einen bestimmten Ordner im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.
 - Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es

empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

3. Klicken Sie auf den entsprechenden  **Hinzufügen**-Link.

Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an. Um einen Server aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die entsprechende  **Löschen**-Schaltfläche.

- Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.
- **Ausschlüsse.** Sie können entweder die im Bereich **Malware-Schutz > Ausschlüsse** der aktuellen Richtlinie definierten Ausschlüsse verwenden oder für die aktuelle Scan-Aufgabe benutzerdefinierte Ausschlüsse definieren. Weitere Informationen finden Sie unter „**Ausschlüsse**“ (S. 301).

Geräte-Scan

Sie können festlegen, dass der Sicherheitsagent externe Speichermedien automatisch erkennt und scannt, sobald diese mit dem Endpunkt verbunden werden. Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- Geräte mit mehr als einer bestimmten Menge gespeicherter Daten.

Bei den Geräte-Scans werden als infiziert erkannte Dateien automatisch desinfiziert oder, falls eine Desinfektion nicht möglich ist, in die Quarantäne verschoben. Einige Geräte wie CDs oder DVDs sind natürlich schreibgeschützt. Auf solchen Speichermedien kann für infizierte Dateien keine Aktion durchgeführt werden.



Beachten Sie

Der Benutzer kann während eines Geräte-Scans weiterhin auf alle Daten auf dem Gerät zugreifen.

Wenn Warnfenster unter **Allgemein > Benachrichtigungen** aktiviert wurden, wird der Benutzer zunächst gefragt, ob ein erkanntes Gerät gescannt werden soll. Es erfolgt kein automatischer Scan.

Wenn ein Geräte-Scan beginnt:

- Ein Benachrichtigungsfenster informiert den Benutzer über den Geräte-Scan, sofern Benachrichtigungsfenster unter **Allgemein > Benachrichtigungen** aktiviert wurden.

Nach Abschluss des Scans muss der Benutzer eventuell erkannte Bedrohungen überprüfen.

Wählen Sie die **Geräte-Scan**-Option, um die automatische Erkennung und Prüfung von Speichergeräten zu aktivieren. Mit den folgenden Optionen können Sie den Geräte-Scan für jeden Gerätetyp individuell festlegen:

- **CD-/DVD-Datenträger**
- **USB-Speichergeräte**
- **Keine Geräte scannen, die mehr Daten gespeichert haben als (MB)**. Mit dieser Option können Sie die Scans von erkannten Geräten automatisch überspringen, wenn die darauf gespeicherten Daten einen festgelegten Umfang überschreiten. Geben Sie das Grössenlimit (in MB) in das entsprechende Feld ein. Null bedeutet, dass kein Grössenlimit angegeben wurde.

HyperDetect



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server
- Linux

HyperDetect bietet eine über die bestehenden Scan-Techniken (Zugriff-, Bedarf- und Datenverkehr-Scan) hinaus eine weitere Sicherheitsschicht zur Abwehr neuer Cyber-Gefahren wie APTs (Advanced Persistent Threats). HyperDetect erweitert die Module Malware-Schutz und Inhaltssteuerung um leistungsstarke Heuristiken, die auf künstlicher Intelligenz und maschinellem Lernen basieren.

HyperDetect ist in der Lage, gezielte Angriffe vorherzusehen und die meisten hochentwickelten Malware-Sorten noch vor der Ausführung zu erkennen, und ist damit deutlich schneller in der Abwehr von Cyber-Gefahren als Signatur- oder Verhaltens-basierte Scan-Technologien.

So konfigurieren Sie HyperDetect:

1. Über das Kästchen **HyperDetect** können Sie das Modul ein- und ausschalten.
2. Wählen Sie die Bedrohungstypen, vor denen Sie Ihr Netzwerk schützen möchten. Standardmäßig ist der Schutz vor allen Bedrohungstypen aktiviert: gezielte Angriffe, verdächtige Dateien und Netzwerkverkehr, Exploits, Ransomware und [Grayware](#).

**Beachten Sie**

Damit die Heuristiken für den Netzwerkverkehr funktionieren, müssen **Inhaltssteuerung > Datenverkehr-Scan** aktiviert sein.

3. Sie können die Sicherheitsstufe für Bedrohungen der ausgewählten Typen anpassen.

Über den Hauptschalter oben an der Bedrohungsliste können Sie eine einheitliche Sicherheitsstufe für alle Bedrohungstypen festlegen, Sie können aber auch für jeden Typ eine eigene Stufe einstellen.

Wenn Sie in diesem Modul eine bestimmte Stufe einstellen, werden bis zu dieser Stufe Aktionen ausgeführt. Wenn Sie als Sicherheitsstufe z. B. **Normal** einstellen, erkennt und blockiert das Modul Bedrohungen, die die Stufen **Tolerant** und **Normal** auslösen würden, aber nicht solche, die nur die Stufe **Aggressiv** auslösen würden.

Tolerant bietet die geringste Sicherheit, **Aggressiv** die höchste.

Bei aggressiver Erkennung sind Fehlalarme möglich, bei toleranter bestehen gewisse Risiken für Ihr Netzwerk. Es wird empfohlen, die Sicherheitsstufe zunächst auf das Maximum einzustellen und dann nach und nach herunterzuregeln, falls Sie zu viele Fehlalarme bekommen.

**Beachten Sie**

Immer wenn Sie den Schutz vor einem Bedrohungstyp aktivieren, wird die entsprechende Sicherheitsstufe auf den Standardwert (**Normal**) gesetzt.

4. Im Bereich **Aktionen** können Sie festlegen, wie HyperDetect auf Funde reagieren soll. Über die Optionen im Klappmenü können Sie die Aktionen festlegen, die bei einem Fund ausgeführt werden sollen:
 - Für Dateien: Zugriff verweigern, desinfizieren, löschen, in die Quarantäne verschieben oder einfach die Datei melden.

- Für Netzwerkverkehr: verdächtigen Datenverkehr blockieren oder einfach melden.
5. Markieren Sie das Kästchen **Berichterstellung für höhere Stufen** neben dem Klappenmenü, wenn Sie Bedrohungen anzeigen möchten, die erst bei höheren Stufen als der eingestellten gefunden würden.

Wenn Sie sich unsicher sind, ob die aktuellen Einstellungen sinnvoll sind, können Sie über einen Klick auf die Schaltfläche **Standard wiederherstellen** unten auf der Seite die Standardeinstellungen wiederherstellen.

Erweiterter Exploit-Schutz



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations

Der erweiterte Exploit-Schutz ist eine proaktive Technologie, die Exploits in Echtzeit erkennt. Aufbauend auf maschinellen Lernverfahren schützt es vor einer Vielzahl an bekannten und unbekanntem Schwachstellen, einschließlich dateiloser Angriffe auf den Speicher.

Markieren Sie das Kontrollkästchen **Erweiterter Exploit-Schutz**, um den Exploit-Schutz zu aktivieren.

Der erweiterte Exploit-Schutz ist auf die empfohlenen Einstellungen voreingestellt. Sie können den Schutz bei Bedarf entsprechend anpassen. Um die Grundeinstellungen wiederherzustellen, klicken Sie rechts neben der Abschnittsüberschrift auf den Link **Auf Standard zurücksetzen**.

Die Einstellungen für den Exploit-Schutz sind in GravityZone in drei Abschnitte unterteilt:

- **Systemweite Funde**

Die Anti-Exploit-Verfahren in diesem Abschnitt überwachen die Systemprozesse, die Ziele von Exploits sind.

Weitere Informationen zu den verfügbaren Verfahren und zur Konfiguration ihrer Einstellungen finden Sie unter [„Systemweite Risikominimierung konfigurieren“](#) (S. 294).

- **Vordefinierte Anwendungen**

Das Modul für den erweiterten Exploit-Schutz ist mit einer Liste der gängigen Anwendungen wie Microsoft Office, Adobe Reader oder Flash Player vorkonfiguriert, die am häufigsten von Exploits betroffen sind.

Weitere Informationen zu den verfügbaren Verfahren und zur Konfiguration ihrer Einstellungen finden Sie unter [„Anwendungsspezifische Verfahren konfigurieren“](#) (S. 295).

● **Weitere Anwendungen**

In diesem Abschnitt können Sie den Schutz für beliebig viele weitere Anwendungen hinzufügen und konfigurieren.

Weitere Informationen zu den verfügbaren Verfahren und zur Konfiguration ihrer Einstellungen finden Sie unter [„Anwendungsspezifische Verfahren konfigurieren“](#) (S. 295).

Sie können jeden Abschnitt durch Anklicken der Überschrift auf- oder zuklappen. Auf diese Weise gelangen Sie schnell zu den Einstellungen, die Sie konfigurieren möchten.

Systemweite Risikominimierung konfigurieren

In diesem Abschnitt sind die folgenden Optionen verfügbar:

Verfahren	Beschreibung
Ausweitung von Benutzerrechten	Verhindert, dass Prozesse unbefugte Berechtigungen und Zugriff auf Ressourcen erhalten. Standardaktion: Beendet den Prozess
LSASS-Prozessschutz	Schützt den LSASS-Prozess vor der Offenlegung von Geheimnissen wie Passworthashes und Sicherheitseinstellungen. Standardaktion: Blockiert den Prozess

Diese Anti-Exploit-Verfahren sind standardmäßig aktiviert. Deaktivieren Sie das entsprechende Kontrollkästchen, um sie zu deaktivieren.

Alternativ können Sie die automatisch durchgeführte Aktion auch zum Zeitpunkt der Erkennung ändern. Wählen Sie eine Aktion, die im zugehörigen Menü verfügbar ist:

- **Prozess beenden:** Beendet den vom Exploit betroffenen Prozess sofort.

- **Prozess blockieren:** Verhindert, dass der bössartige Prozess unbefugt auf Ressourcen zugreift.
- **Nur Bericht:** GravityZone meldet das Ereignis, ohne Abhilfemaßnahmen zu ergreifen. Sie können die Ereignisdetails in der Benachrichtigung **Erweiterter Exploit-Schutz** sowie in den Berichten Blockierte Anwendungen und Sicherheitsüberprüfung einsehen.

Anwendungsspezifische Verfahren konfigurieren

Auf die vordefinierten und weiteren Anwendungen werden die gleichen Anti-Exploit-Verfahren angewandt. Sie werden im Folgenden beschrieben:

Verfahren	Beschreibung
ROP-Emulation	Erkennt Versuche, die Speicherseiten für Daten mit Hilfe des ROP-Verfahrens (Return-Oriented Programming) ausführbar zu machen. Standardaktion: Prozess beenden
ROP-Stack-Pivoting	Erkennt Versuche, den Codefluss mithilfe des ROP-Verfahrens durch zu übernehmen, indem die Stapelposition überprüft wird. Standardaktion: Prozess beenden
ROP - unerlaubter Aufruf	Erkennt Versuche, den Codefluss mithilfe des ROP-Verfahrens durch zu übernehmen, indem die Aufrufer sensibler Systemfunktionen überprüft werden. Standardaktion: Prozess beenden
ROP - Stackfehlausrichtung	Erkennt Versuche, den Codefluss mithilfe des ROP-Verfahrens durch zu übernehmen, indem der Stapeladressabgleich überprüft wird. Standardaktion: Prozess beenden
ROP Return To Stack	Erkennt Versuche, Code direkt auf dem Stapel mit Hilfe der ROP-Technik auszuführen, indem der Adressbereich der Rückgabe überprüft wird. Standardaktion: Prozess beenden

Verfahren	Beschreibung
ROP Stack ausführbar machen	Erkennt Versuche, den Stapel mithilfe der ROP-Technik zu beschädigen, indem der Schutz der Stapelseiten überprüft wird. Standardaktion: Prozess beenden
Flash - allgemein	Erkennt Flash Player-Exploit-Versuche. Standardaktion: Prozess beenden
Flash-Payload	Erkennt Versuche, böartigen Code in Flash Player auszuführen, indem es Flash-Objekte im Speicher scannt. Standardaktion: Prozess beenden
VBScript Generic	Erkennt VBScript-Exploit-Versuche. Standardaktion: Prozess beenden
Shellcode-Ausführung	Erkennt Versuche, mithilfe von Shellcode neue Prozesse zu erstellen oder Dateien herunterzuladen. Standardaktion: Prozess beenden
Shellcode LoadLibrary	Erkennt Versuche, mithilfe von Shellcode Code über Netzwerkpfade auszuführen. Standardaktion: Prozess beenden
Anti-Detour	Erkennt Versuche, Sicherheitschecks bei der Erstellung neuer Prozesse zu umgehen. Standardaktion: Prozess beenden
Shellcode EAF (Export Address Filtering)	Erkennt Versuche von böartigem Code, über DLL-Exporte auf sensible Systemfunktionen zuzugreifen. Standardaktion: Prozess beenden
Shellcode Thread	Erkennt Versuche, böartigen Code einzuspeisen, indem neu erstellte Threads überprüft werden. Standardaktion: Prozess beenden
Anti-Meterpreter	Erkennt Versuche, eine umgekehrte Shell zu erstellen, indem ausführbare Speicherseiten gescannt werden. Standardaktion: Prozess beenden

Verfahren	Beschreibung
Erstellung eines obsoleten Prozesses	Erkennt Versuche, neue Prozesse mit veralteten Verfahren zu erstellen. Standardaktion: Prozess beenden
Erstellung eines Kindprozesses	Blockiert die Erstellung von Kindprozessen. Standardaktion: Prozess beenden
Windows DEP erzwingen	Erzwingt Data Execution Prevention (DEP), um die Ausführung von Code von Datenseiten zu blockieren. Standard: Deaktiviert
Modulumzug erzwingen (ASLR)	Verhindert das Laden von Code an vorhersehbaren Stellen, indem Speichermodule verschoben werden. Standard: Aktiviert
Emerging Exploits	Schützt vor neuen und aufkommenden Bedrohungen und Exploits. Schnelle Updates werden für diese Kategorie verwendet, bevor umfangreichere Änderungen vorgenommen werden können. Standard: Aktiviert

Um andere Anwendungen als die vordefinierten zu überwachen, klicken Sie auf die Schaltfläche **Anwendung hinzufügen** oben oder unten auf der Seite.

So können Sie die Anti-Exploit-Einstellungen für eine Anwendung konfigurieren:

1. Klicken Sie bei bestehenden Anwendungen auf den Namen der Anwendung. Klicken Sie bei neuen Anwendungen auf die Schaltfläche **Hinzufügen**.

Auf einer neuen Seite werden alle Verfahren und deren Einstellungen für die ausgewählte Anwendung angezeigt.



Wichtig

Lassen Sie Vorsicht walten, wenn Sie neue Anwendungen zur Überwachung hinzufügen. Bitdefender kann nicht garantieren, dass die Kompatibilität mit allen Anwendungen gewährleistet ist. Es empfiehlt sich daher, die Funktion zunächst auf einigen nicht kritischen Endpunkten zu testen und dann erst im Netzwerk einzusetzen.

2. Wenn Sie eine neue Anwendung hinzufügen, geben Sie ihren Namen und die Namen ihrer Prozesse in die dafür vorgesehenen Felder ein. Verwenden Sie das Semikolon (;), um Prozessnamen zu trennen.
3. Wenn Sie die Beschreibung eines Verfahrens schnell überprüfen möchten, klicken Sie auf den Pfeil neben dem Namen.
4. Aktivieren oder deaktivieren Sie bei Bedarf die Kontrollkästchen der Exploit-Verfahren.

Verwenden Sie die Option **Alle**, wenn Sie alle Verfahren auf einmal markieren möchten.

5. Bei Bedarf können Sie die automatische Aktion zum Zeitpunkt der Erkennung ändern. Wählen Sie eine Aktion, die im zugehörigen Menü verfügbar ist:
 - **Prozess beenden:** Beendet den vom Exploit betroffenen Prozess sofort.
 - **Nur Bericht:** GravityZone meldet das Ereignis, ohne Abhilfemaßnahmen zu ergreifen. Sie können die Ereignisdetails in der Benachrichtigung **Erweiterter Exploit-Schutz** und in den Berichten einsehen.

Standardmäßig sind alle Verfahren für vordefinierte Anwendungen so eingestellt, dass dem Problem entgegengewirkt wird, während für weitere Anwendungen nur das Ereignis gemeldet wird.

Um die Aktion für alle Verfahren auf einmal zu ändern, wählen Sie die Aktion aus dem Menü der Option **Alle**.

Klicken Sie oben auf der Seite auf die Schaltfläche **Zurück**, um zu den allgemeinen Einstellungen des Exploit-Schutzes zurückzukehren.

Einstellungen

In diesem Bereich können Sie die Quarantäne-Einstellungen und die Regeln für Scan-Ausschlüsse festlegen.

- [Quarantäne-Einstellungen konfigurieren](#)
- [Konfiguration der Scan-Ausschlüsse](#)

Quarantäne

Für die von den Zielendpunkten in die Quarantäne verschobenen Dateien können Sie die folgenden Optionen konfigurieren:

- **Delete files older than (days).** Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Quarantäne-Dateien an das Bitdefender-Labor senden, jeweils alle (Stunden).** Standardmäßig werden in die Quarantäne verschobene Dateien automatisch stündlich an die Bitdefender-Labors gesandt. Sie können das Intervall einstellen, in dem in die Quarantäne verschobene Dateien gesendet werden (standardmäßig 1 Stunde). Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.
- **Quarantäne nach Signaturen-Update erneut scannen.** Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Sicherheitsinhalte zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.
- **Dateien vor der Desinfektion in die Quarantäne kopieren.** Aktivieren Sie diese Option, um im Falle von Fehlalarmen Datenverlust zu vermeiden, indem als infiziert erkannte Dateien vor der Desinfektion in die Quarantäne kopiert werden. Später können Sie unbedenkliche Dateien von der Seite **Quarantäne** aus wiederherstellen.
- **Benutzern erlauben, Aktionen in der lokalen Quarantäne auszuführen.** Diese Option steuert die Aktionen, die von den Endpunktbenutzern über die Bitdefender Endpoint Security Tools-Benutzeroberfläche für die Dateien in der lokalen Quarantäne ausgeführt werden dürfen. Lokale Benutzer können über die in Bitdefender Endpoint Security Tools verfügbaren Optionen die Dateien in Quarantäne standardmäßig auf ihrem Computer wiederherstellen oder löschen. Wird diese Option deaktiviert, können die Benutzer über die Bitdefender Endpoint Security Tools-Benutzeroberfläche nicht mehr auf die interaktiven Schaltflächen für die Dateien in Quarantäne zugreifen.

Zentrale Quarantäne

Falls Sie die Dateien in Quarantäne von Ihren verwalteten Endpunkten für die weitere Analyse behalten möchten, nutzen Sie die Option **Zentrale Quarantäne**. So wird eine archivierte Kopie jeder lokalen Datei, die in die Quarantäne verschoben wird, an eine Netzwerkfreigabe übermittelt.

Nach Aktivierung dieser Option wird jede Datei, die von den verwalteten Endpunkten in die Quarantäne verschoben wird, kopiert und in einem passwortgeschützten ZIP-Archiv auf der angegebenen Netzwerkadresse gespeichert. Für den Archivnamen wird der Hash der Datei in Quarantäne verwendet.



Wichtig

Die Größenbeschränkung für das Archiv ist 100 MB. Wird die Größenbeschränkung von 100 MB überschritten, wird das Archiv nicht unter der Netzwerkadresse gespeichert.

Füllen Sie die folgenden Felder aus, um die Einstellungen für die Zentrale Quarantäne zu konfigurieren:

- **Archiv-Passwort:** Geben Sie das Passwort ein, das für das Quarantäne-Archiv benötigt wird. Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten. Geben Sie das Passwort im nächsten Feld erneut ein.
- **Pfad der Freigabe:** Geben Sie hier den Netzwerkpfad ein, unter dem Sie die Archive speichern möchten (z. B. `\\Computer\Ordner`).
- Zur Verbindung mit der Netzwerkfreigabe benötigter Benutzername und Passwort. Für die Benutzernamen werden folgende Formate unterstützt:
 - `Benutzername@Domain`
 - `Domain\Benutzername`
 - `Benutzername.`

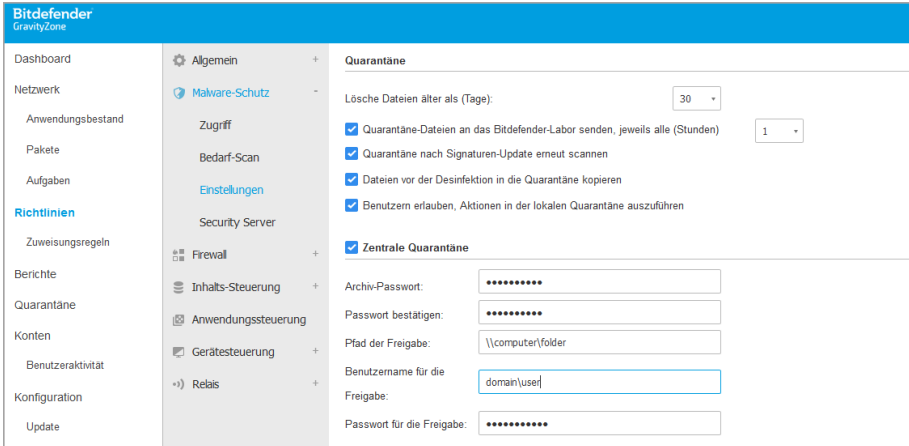
Zur ordnungsgemäßen Funktion der zentralen Quarantäne müssen die folgenden Bedingungen erfüllt sein:

- Auf den freigegebenen Speicherort kann über das Netzwerk zugegriffen werden.
- Die Endpunkte sind mit der Netzwerkfreigabe verbunden.
- Die Anmeldedaten sind gültig und ermöglichen den Schreibzugriff auf die Netzwerkfreigabe.
- Die Netzwerkfreigabe verfügt über ausreichend Speicherplatz.



Beachten Sie

Die zentrale Quarantäne gilt nicht für die Mail-Server-Quarantäne.



Zentrale Quarantäne

Wenn Sie im Abschnitt **Sandbox Analyzer > Endpunktsensor** eine lokale Sandbox Analyzer-Instanz konfiguriert haben, können Sie das Kontrollkästchen **Objekte aus der Quarantäne automatisch an einen Sandbox Analyzer übermitteln** markieren. Bitte beachten Sie, dass die übermittelten Objekte eine Größe von 50 MB nicht überschreiten dürfen.

Ausschlüsse

Der Bitdefender-Sicherheitsagent kann bestimmte Objekttypen vom Scan ausschließen. Anti-Malware-Ausschlüsse sollten unter besonderen Umständen eingesetzt werden oder wenn dies von Microsoft oder Bitdefender empfohlen wird. Eine aktualisierte Liste der von Microsoft empfohlenen Ausschlüsse finden Sie in diesem [Artikel](#).

In diesem Bereich können Sie die Verwendung verschiedener Arten von Ausschlüssen im Bitdefender-Sicherheitsagent konfigurieren.

- **Eingebaute Ausschlüsse** sind standardmäßig aktiviert und im Bitdefender-Sicherheitsagenten enthalten.

Wenn Sie alle Objekttypen scannen möchten, können Sie eingebaute Ausschlüsse deaktivieren, dies wird sich aber erheblich auf die Leistung der Maschine und die Dauer des Scans auswirken.

- Sie können nach Bedarf auch **Benutzerdefinierte Ausschlüsse** für selbst entwickelte Anwendungen oder benutzerdefinierte Tools festlegen.

Benutzerdefinierte Anti-Malware-Ausschlüsse gelten für eine oder mehrere der folgenden Scan-Methoden:

- Zugriff-Scan
- Bedarf-Scan
- Advanced Threat Control
- Schutz vor dateilosen Angriffen
- Ransomware-Abhilfemaßnahme



Wichtig

- Sollten Sie eine EICAR-Testdatei verwenden, um den Malware-Schutz regelmäßig zu überprüfen, sollten Sie diese von den Zugriff-Scans ausschließen.
- Wenn Sie VMware Horizon View 7 und App Volumes AppStacks verwenden, lesen Sie sich bitte dieses [VMware-Dokument](#) durch.

Um bestimmte Objekte vom Scan auszuschließen, wählen Sie die Option **Benutzerdefinierte Ausschlüsse** und fügen Sie die Regeln in die darunterliegende Tabelle ein.

The screenshot shows the 'Quarantäne' settings in Bitdefender GravityZone. On the left is a navigation menu with options like 'Allgemein', 'Malware-Schutz', 'Zugriff', 'Bedarf-Scan', 'Einstellungen', 'Firewall', 'Inhalts-Steuer.', 'Gerätesteuerung', and 'Relais'. The main area is titled 'Quarantäne' and contains several settings: 'Lösche Dateien älter als (Tage):' set to 30; three checked options: 'Quarantäne-Dateien an das Bitdefender-Labor senden...', 'Quarantäne nach Signaturen-Update erneut scannen', and 'Dateien vor der Desinfektion in die Quarantäne kopieren'; and two checked exclusion options: 'Eingebaute Ausschlüsse' and 'Benutzerdefinierte Ausschlüsse'. The 'Benutzerdefinierte Ausschlüsse' option is highlighted with a red box. Below these options is a table with columns: 'Typ', 'Dateien, Ordner, Dateiendungen oder Prozesse', 'Module', and 'Aktion'. The table contains one entry: 'Datei' (with a dropdown arrow), 'Bestimmte Pfade' (with a dropdown arrow), 'Bedarf-Scan' (with a dropdown arrow), and a plus sign in a circle.

Richtlinien für Computer und virtuelle Maschinen – Benutzerdefinierte Ausschlüsse

So fügen Sie eine Regel für benutzerdefinierte Ausschlüsse hinzu:

1. Wählen Sie die Art des Ausschlusses aus dem Menü:

- **Datei:** Nur die angegebene Datei
- **Ordner:** Alle Dateien und Prozesse im angegebenen Ordner sowie in allen Unterordnern
- **Dateiendung:** Alle Objekte mit der angegebenen Dateiendung
- **Prozess:** Jedes Objekt, auf das der ausgeschlossene Prozess zugreift
- **Datei-Hash:** Die Datei mit dem angegebenen Hash-Wert
- **Zertifikat-Hash:** Alle Anwendungen unter dem angegebenen Zertifikat-Hash (Fingerabdruck)
- **Name der Bedrohung:** Jedes Objekt mit dem Namen des Fundes (nicht verfügbar für Linux-Betriebssysteme)
- **Befehlszeile:** die angegebene Befehlszeile (nur für Windows-Betriebssysteme verfügbar)



Warnung

In mit vShield integrierten VMware-Umgebungen ohne Agent lassen sich nur Ordner und Endungen ausschließen. Durch Installation von Bitdefender Tools auf virtuellen Maschinen können Sie auch Dateien und Prozesse ausschließen. Während der Konfiguration des Pakets wählen Sie das Kästchen **Endpunkt mit vShield installieren, wenn eine mit vShield integrierte VMware-Umgebung erkannt wird**. Weitere Informationen erhalten Sie im Abschnitt **Installationspaket erstellen** der Installationsanleitung.

2. Geben Sie die für die ausgewählte Ausschlussart spezifischen Details an:

Datei, Ordner oder Prozess

Geben Sie den Pfad zu dem Objekt ein, das vom Scan ausgeschlossen werden soll. Es gibt eine Reihe hilfreicher Optionen zum Schreiben des Pfads:

- Geben Sie den Pfad explizit an.

Zum Beispiel: C: emp

Um Ausschlüsse für UNC-Pfade hinzuzufügen, verwenden Sie eine der folgenden Syntaxen:

```
\\hostname\shareName\filePath
```

```
\\IPaddress\shareName\filePath
```

- Verwenden Sie die im Dropdown-Menü verfügbaren Systemvariablen.

Bei Prozessausschlüssen müssen Sie auch den Namen der ausführbaren Datei der Anwendung angeben.

Zum Beispiel:

%ProgramFiles% - Schließt den Ordner Programme aus.

%WINDIR%\system32 - Schließt den Ordner system32 im Windows-Ordner aus.



Beachten Sie

Es empfiehlt sich, (nach Möglichkeit) [Systemvariablen](#) zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

- Verwenden Sie Platzhalter.

Ein Sternchen (*) ersetzt null oder mehr Zeichen. Ein Fragezeichen (?) ersetzt genau ein Zeichen. Sie können mehrere Fragezeichen benutzen,

um eine beliebige Kombination einer bestimmten Anzahl von Zeichen zu ersetzen. So steht ??? z. B. für eine beliebige Folge von genau drei Zeichen.

Zum Beispiel:

Dateiausschlüsse:

`C:\Test*` - Schließt alle Dateien im Ordner Test aus.

`C:\Test*.png` – Schließt alle PNG-Dateien im Ordner Test aus.

Ordnerausschlüsse:

`C:\Test*` - schließt alle Ordner im Ordner Test aus

Prozessausschlüsse:

`C:\Program Files\WindowsApps\Microsoft.Not?.exe` - Schließt Microsoft Notes-Prozesse aus.



Beachten Sie

Prozessausschlüsse unterstützen keine Platzhalter auf Linux-Betriebssystemen.

Dateiendung

Geben Sie eine oder mehrere Dateiendungen ein, die vom Scan ausgeschlossen werden sollen, und trennen Sie sie durch ein Semikolon ";". Sie können die Endungen dabei mit oder ohne den führenden Punkt eingeben. Geben Sie zum Beispiel die Endung `txt` ein, um Textdateien auszuschließen.



Beachten Sie

Auf Linux-Systemen wird bei Dateierweiterungen zwischen Groß- und Kleinschreibung unterschieden, wodurch Dateien mit dem gleichen Namen und unterschiedlichen Erweiterungen wie separate Objekte behandelt werden. So unterscheidet sich z. B. `file.txt` von `file.TXT`.

Datei-Hash, Zertifikat-Hash, Bedrohungsname oder Befehlszeile

Geben Sie je nach Ausschlussregel den Dateihash, den Zertifikatsfingerabdruck (Hash), den genauen Namen der Bedrohung oder die Befehlszeile ein. Sie können ein Objekt pro Ausschluss verwenden.

3. Wählen Sie die Scan-Methoden, auf die die Regel angewendet werden soll. Einige Ausschlüsse sind möglicherweise nur für Zugriff-Scans, Bedarf-Scans

oder ATC/IDS von Bedeutung und andere empfehlen sich unter Umständen für alle drei Module.

4. Klicken Sie optional auf die Schaltfläche **Hinweise anzeigen**, um in der Spalte **Hinweise** eine Notiz zu der Regel hinzuzufügen.
5. Klicken Sie auf den Button **+Hinzufügen**.

Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu löschen, klicken Sie auf den entsprechenden **Löschen**-Link.



Wichtig

Bitte beachten Sie, dass Ausschlüsse für Bedarf-Scans bei Kontext-Scans NICHT berücksichtigt werden. Klicken Sie mit der rechten Maustaste auf eine Datei oder einen Ordner und wählen Sie **Mit Bitdefender Endpoint Security Tools scannen**, um einen Kontext-Scan zu starten.

Importieren und Exportieren von Ausschlüssen

Wenn Sie Ausschlussregeln in mehreren Richtlinien wiederverwenden möchten, können Sie sie exportieren und wieder importieren.

So exportieren Sie benutzerdefinierte Ausschlüsse:

1. Klicken Sie dazu oben an der Ausschlusstabelle auf **Exportieren**.
2. Speichern Sie die CSV-Datei auf Ihrem Computer. Je nach den Browser-Einstellungen wird die Datei automatisch heruntergeladen oder Sie werden aufgefordert, einen Speicherort für sie zu wählen.

Jede Zeile in der CSV-Datei entspricht einer einzelnen Regel mit den Feldern in der folgenden Reihenfolge:

```
<exclusion type>, <object to be excluded>, <modules>
```

Dies sind die möglichen Werte für die CSV-Felder:

Ausschlussart:

- 1 für Dateiausschlüsse
- 2 für Ordnerausschlüsse
- 3 für Endungsausschlüsse

- 4 für Prozessausschlüsse
- 5, für Datei-Hash-Ausschlüsse
- 6, für Zertifikat-Hash-Ausschlüsse
- 7, für Bedrohungsnamen-Ausschlüsse
- 8, für Befehlszeilen-Ausschlüsse

Auszuschließendes Objekt:

Ein Pfad oder eine Dateierdung

Module:

- 1 für Bedarf-Scans
- 2 für Zugriff-Scans
- 3 für alle Module
- 4 für ATC/IDS

Eine CSV-Datei, die Malware-Schutz-Ausschlüsse enthält, könnte zum Beispiel so aussehen:

```
1, "d:\\temp", 1
1, %WinDir%, 3
4, "%WINDIR%\\system32", 4
```

**Beachten Sie**

Windows-Pfade müssen einen doppelten Backslash (\) haben. Zum Beispiel %WinDir%\\System32\\LogFiles.

So importieren Sie benutzerdefinierte Ausschlüsse:

1. Klicken Sie auf **Importieren**. Das Fenster **Richtlinienausschlüsse importieren** wird geöffnet.
2. Klicken Sie auf **Hinzufügen** und wählen Sie dann die CSV-Datei.
3. Klicken Sie auf **Speichern**. Die Tabelle wird mit den gültigen Regeln gefüllt. Wenn eine CSV-Datei ungültige Regeln enthält, werden Sie durch eine Meldung auf die entsprechenden Zeilennummern hingewiesen.

Security Server

In diesem Bereich können Sie Folgendes konfigurieren:

- [Security Server-Zuweisung](#)
- [Security Server-spezifische Einstellungen](#)

Richtlinie – Computer und virtuelle Maschinen – Malware-Schutz – Security-Server

Security Server-Zuweisung

Sie können den gewünschten Endpunkten beliebig viele Security Server zuweisen und die Prioritäten festlegen, anhand derer die Endpunkte einen Security Server für den Versand von Scan-Anfragen auswählen.



Beachten Sie

Wir empfehlen, virtuelle Maschinen und Computer mit geringen Ressourcen über Security Server zu scannen.

Wenn Sie den gewünschten Endpunkten einen Security Server zuweisen möchten, fügen Sie den gewünschten Security Server wie folgt in der der Tabelle **Security Server-Zuweisung** hinzu:

1. Klicken Sie auf das **Security Server**-Klappmenü und wählen Sie einen Security Server.

2. Wenn sich der Security Server in einer DMZ oder hinter einem NAT-Server befindet, geben Sie die FQDN oder IP-Adresse des NAT-Servers in das Feld **Benutzerdefinierter Servername/IP** ein.

**Wichtig**

Vergewissern Sie sich, dass die Port-Weiterleitung auf dem NAT-Server richtig konfiguriert ist, damit der Datenverkehr von den Endpunkten den Security Server erreichen kann.

3. Klicken Sie in der Spalte **Aktionen** auf die Schaltfläche **Hinzufügen**.
Der Security Server wird der Liste hinzugefügt.
4. Wiederholen Sie diese Schritte, wenn Sie andere Security Server hinzufügen möchten, falls nötig und möglich.

So legen Sie die Priorität der Security Server fest:

1. Über die Pfeile in der Spalte **Aktionen** können Sie die Priorität der Security Server hoch und runter setzen.

Wenn Sie mehrere Security Server zuweisen, hat der am weitesten oben stehende die höchste Priorität und wird zuerst ausgewählt. Wenn dieser Security Server nicht erreichbar oder überlastet ist, wird der nächste Security Server aus der Liste ausgewählt. Der Scan-Datenverkehr wird zum ersten Security Server geleitet, der verfügbar ist und eine passende Auslastung aufweist.

2. Wählen Sie die Option **Wenn möglich, zuerst mit dem Security Server verbinden, der auf demselben physischen Host installiert ist, unabhängig von der zugewiesenen Priorität.**, um die Endpunkte gleichmäßig aufzuteilen und die Latenz zu optimieren. Wenn dieser Security Server nicht erreichbar ist, wird der nächste Security Server aus der Liste ausgewählt.

**Wichtig**

Diese Option funktioniert nur bei Security Server Multi-Platform nur, wenn GravityZone mit der virtuellen Umgebungen integriert ist.

Um einen Security Server aus der Liste zu entfernen, klicken Sie auf die entsprechende **Löschen**-Schaltfläche in der Spalte **Aktionen**.

Security Server-Einstellungen

Wenn Sie die Richtlinie Security Servern zuweisen, können Sie die folgenden Einstellungen vornehmen:

- **Anzahl der gleichzeitigen Bedarf-Scans beschränken.**

Bei der Ausführung mehrerer Bedarf-Scan-Aufgaben auf virtuellen Maschinen, die sich denselben Datenspeicher teilen, kann es zu einem [Malware-Schutz-Ressourcenkonflikt](#) kommen. Um das zu verhindern, sollten Sie nur eine bestimmte Anzahl an gleichzeitig laufenden Scan-Aufgaben zulassen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie die Option **Anzahl der gleichzeitigen Bedarf-Scans beschränken**.
2. Wählen Sie die gewünschte Anzahl gleichzeitig möglicher Scan-Aufgaben aus dem Klappmenü. Sie können eine vordefinierte Stufe wählen oder selbst einen Wert eingeben.

Die Formel für die Anzahl gleichzeitig erlaubter Scan-Aufgaben für die einzelnen vordefinierten Stufen lautet: $N = a \times \text{MAX}(b ; v\text{CPUs} - 1)$.

Hierbei gilt:

- N = Anzahl gleichzeitig erlaubter Scan-Aufgaben
- a = Koeffizient mit folgenden Werten: 1 - für Gering; 2 - für Mittel; 4 - für Hoch
- $\text{MAX}(b ; v\text{CPU}-1)$ = eine Funktion, die die Höchstzahl verfügbarer Scan-Slots auf dem Security Server zurückgibt.
- b = die Standardanzahl an Bedarf-Scan-Slots (derzeit 4).
- $v\text{CPU}s$ = Anzahl der virtuellen CPUs, die dem Security Server zugewiesen sind

Zum Beispiel:

Für einen Security Server mit 12 CPUs und der Begrenzungsstufe „Hoch“ für gleichzeitig erlaubte Scans kommen wir auf eine Maximalanzahl von:

$N = 4 \times \text{MAX}(4 ; 12-1) = 4 \times 11 = 44$ gleichzeitige Bedarf-Scan-Aufgaben.

- **Affinitätsregeln für Security Server Multi-Plattform aktivieren**

Wählen Sie, wie sich der Security Server verhalten soll, wenn sein Host in den Wartungsmodus geht:

- Wenn die Option aktiviert ist, bleibt der Security Server an den Host gebunden und wird von GravityZone abgeschaltet. Wenn die Wartung beendet ist, startet GravityZone den Security Server automatisch neu.

Dies ist das Standardverhalten.

- Wenn die Option deaktiviert ist, wird der Security Server auf einen anderen Host verschoben und läuft weiter. In diesem Fall ändert sich der Name des Security Server im Control Center und verweist auf den ursprünglichen Host. Diese Namensänderung bleibt bestehen, bis der Security Server auf seinen ursprünglichen Host zurück verschoben wurde.

Wenn genügend Ressourcen zur Verfügung stehen, kann der Security Server auf einen Host verschoben werden, auf dem bereits ein anderer Security Server installiert ist.



Wichtig

Diese Option ist wirkungslos, wenn der Security Server auch von HVI verwendet wird.

● SSL verwenden

Markieren Sie diese Option, wenn Sie die Verbindung zwischen den Endpunkten und den angegebenen Security Server-Appliances verschlüsseln möchten.

Standardmäßig verwendet GravityZone selbst unterzeichnete Sicherheitszertifikate. Sie können sie auf der Seite **Konfiguration > Zertifikate** des Control Center durch Ihre eigenen Zertifikate ersetzen. Weitere Informationen finden Sie im Kapitel „Konfigurieren der Control Center-Einstellungen“ im Installationshandbuch.

● Kommunikation zwischen Security Servern und GravityZone

Wählen Sie eine der verfügbaren Optionen, um die Proxy-Einstellungen für die Kommunikation zwischen den ausgewählten Security Server-Maschinen und GravityZone definieren:

- **Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.

- **Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- **Proxy nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den Bitdefender-Komponenten kommunizieren.

7.2.4. Sandbox Analyzer



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

Der Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben.

In diesem Abschnitt können Sie Folgendes konfigurieren:

- [Übermittlung über Endpunktsensor](#)
- [Übermittlung über Netzwerksensor](#)
- [Übermittlung über ICAP-Sensor](#)
- [Sandbox Manager-Einstellungen](#)

In den Richtlinieneinstellungen können Sie auch die automatische Übermittlung aus der zentralen Quarantäne konfigurieren. Weitere Einzelheiten dazu finden Sie unter „[Zentrale Quarantäne](#)“ (S. 299).

Informationen zur manuellen Übermittlung finden Sie unter „[Manuelle Übermittlung](#)“ (S. 501). Weitere Informationen zur Übermittlung über die API finden Sie in den Kapiteln **Sandbox** und **Sandbox Portal** im [GravityZone-API-Handbuch \(On-Premises\)](#).

Endpunktsensor

Bitdefender Endpoint Security Tools kann auf Windows-Endpunkten als Einspeisungssensor für Sandbox Analyzer fungieren.

The screenshot shows the configuration page for the 'Sandbox Analyzer' endpoint sensor. The left sidebar lists various security components, with 'Sandbox Analyzer' selected. The main content area is titled 'Computer und virtuelle Maschinen' and contains several sections:

- Allgemein:** A checkbox for 'Automatische Stichproben-Übermittlung von den verwalteten Endpunkten' is checked.
- Malware-Schutz:** A note states that the integrated endpoint sensor sends samples to the Sandbox Analyzer for analysis.
- Analysemodus:** A note explains the two modes: 'Überwachung' (selected) and 'Blockieren'. 'Überwachung' allows users to access objects, while 'Blockieren' prevents access.
- Bereinigungsaktionen:** A note explains the actions for detected threats. Two dropdown menus are shown: 'Standardaktion' set to 'Nur Bericht' and 'Ersatzfunktion' set to 'In Quarant. versch.'.
- Informationen:** A note explains that the reporting target and exclusions are defined in the 'Malware-Schutz' settings.
- Vorabfilterung von Inhalten:** A section for content pre-filtering.

Richtlinien > Sandbox Analyzer > Endpunktsensor

Gehen Sie folgt vor, um die automatische Übermittlung per Endpunktsensor zu konfigurieren:

1. Wählen Sie unter **Verbindungseinstellungen** eine der Optionen aus:

- **Cloud Sandbox Analyzer verwenden** - Abhängig von Ihrem Standort übermittelt der Endpunktsensor Stichproben an die entsprechende von Bitdefender gehostete Sandbox Analyzer-Instanz.
- **Lokale Sandbox Analyzer-Instanz verwenden** - Der Endpunktsensor übermittelt Stichproben an eine Instanz von Sandbox Analyzer On-Premises. Wählen Sie die gewünschte Sandbox Analyzer-Instanz aus dem Dropdown-Menü.

Wenn sich Ihr Netzwerk hinter einem Proxy-Server oder einer Firewall befindet, können Sie das Kästchen **Proxy-Konfiguration verwenden** markieren und dann einen Proxy konfigurieren, um die Verbindung zum Sandbox Analyzer herzustellen.

Sie müssen die folgenden Felder ausfüllen:

- **Server** - die IP-Adresse des Proxy-Servers.
 - **Port** - der Port, über den die Verbindung zum Proxy-Server hergestellt wird.
 - **Benutzername** - ein Benutzername, der vom Proxy erkannt wird.
 - **Passwort** – das gültige Passwort für den entsprechenden Benutzer.
2. Markieren Sie das Kästchen **Automatische Stichproben-Übermittlung von den verwalteten Endpunkten**, um die automatische Übermittlung von verdächtigen Dateien an den Sandbox Analyzer zu erlauben.



Wichtig

- Der Sandbox Analyzer benötigt Zugriff-Scans. Dazu muss das Modul **Malware-Schutz > Zugriff-Scans** aktiviert sein.
 - Der Sandbox Analyzer verwendet dieselben Ziele und Ausschlüsse, die im Modul **Malware-Schutz > Zugriff-Scans** definiert sind. Bei der Konfiguration des Sandbox Analyzer sollten Sie die Zugriff-Scan-Einstellungen sorgfältig überprüfen.
 - Um Fehlalarme (versehentliche Funde legitimer Anwendungen) auszuschließen, können Sie Ausschlüsse über Dateinamen, -erweiterungen, -größen und -pfade einrichten. Weitere Informationen zu Zugriff-Scans finden Sie hier: [„Malware-Schutz“ \(S. 269\)](#).
 - Dateien, die ins Archiv hochgeladen werden, dürfen höchstens 50 MB groß sein.
3. Wählen Sie **Analysemodus**. Es sind zwei Optionen verfügbar:
- **Überwachung**. Der Benutzer kann auf die Datei zugreifen, während sie in der Sandbox analysiert wird, sollte sie aber nicht ausführen, bevor er die Ergebnisse der Analyse erhalten hat.
 - **Blockieren**. Der Benutzer kann die Datei nicht ausführen, bis das Analyseergebnis vom Sandbox Analyzer-Cluster über das Sandbox Analyzer-Portal an den Endpunkt zurückgegeben wird.
4. Legen Sie die **Bereinigungsaktionen** fest. Diese Aktionen werden ausgeführt, wenn der Sandbox Analyzer eine Bedrohung findet. Für jeden Analysemodus können zwei Aktionen festgelegt werden, eine Standardaktion und eine Ersatzaktion. Der Sandbox Analyzer führt zunächst immer die Standardaktion aus. Nur wenn diese nicht vollständig durchgeführt werden kann, führt er die Ersatzaktion aus.

Wenn Sie zum ersten Mal auf diesen Bereich zugreifen, ist Folgendes voreingestellt:



Beachten Sie

Es wird empfohlen, in dieser Konfiguration Bereinigungsaktionen zu verwenden.

- Im **Überwachungsmodus** ist die Standardaktion **Nur Bericht**; Ersatzaktion ist keine eingestellt.
- Im **Blockiermodus** ist die Standardaktion **Quarantäne**, die Ersatzaktion **Löschen**.

Der Sandbox Analyzer stellt Ihnen die folgenden Bereinigungsaktionen zur Auswahl:

- **Desinfizieren**. Dadurch wird der Schad-Code von den infizierten Dateien entfernt.
- **Löschen**. Dadurch wird die gefundene Datei vollständig von der Festplatte gelöscht.
- **Quarantäne**. Dadurch werden gefundene Dateien von ihrem aktuellen Speicherort in den Quarantäneordner verschoben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in der Quarantäne über die **Quarantäne**-Seite im Control Center verwalten.
- **Nur Bericht**. Der Sandbox Analyzer meldet gefundene Bedrohungen nur. Er führt keine Aktionen durch.



Beachten Sie

Je nach Standardaktion kann eventuell keine Ersatzaktion festgelegt werden.

5. Sowohl die Standard- als auch die Ausweich-Wiederherstellungsmaßnahmen sind auf den Modus **Nur Bericht** eingestellt.
6. Passen Sie unter **Vorabfilterung von Inhalten** die Sicherheitsstufe zur Abwehr potenzieller Bedrohungen an. Im Endpunktsensor ist ein Mechanismus zum Filtern von Inhalten eingebettet, der bestimmt, ob eine verdächtige Datei im Sandbox Analyzer detoniert werden muss.

Die folgenden Objekttypen werden unterstützt: Anwendungen, Dokumente, Skripte, Archive, E-Mails. Weitere Informationen zu den unterstützten Objekttypen

finden Sie unter „Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden“ (S. 550).

Über den Hauptschalter oben auf der Bedrohungsliste können Sie eine einheitliche Sicherheitsstufe für alle Objekttypen festlegen, Sie können aber auch für jeden Typ eine eigene Stufe einstellen.

Wenn Sie das Modul auf eine bestimmte Stufe einstellen, führt dies zu einer bestimmten Anzahl von eingereichten Stichproben:

- **Tolerant.** Der Endpunktsensor übermittelt nur die Objekte automatisch an den Sandbox Analyzer, die am wahrscheinlichsten schädlich sind, und ignoriert alle übrigen Objekte.
- **Normal.** Der Endpunktsensor findet ein Gleichgewicht zwischen den übermittelten und ignorierten Objekten und übermittelt sowohl Objekte mit einer hohen und einer geringen Wahrscheinlichkeit, schädlich zu sein, an den Sandbox Analyzer.
- **Aggressiv.** Der Endpunktsensor übermittelt fast alle Objekte an den Sandbox Analyzer, unabhängig von ihrem potenziellen Risiko.

In einem eigenen Feld können Sie Ausnahmen für die Objekttypen festlegen, die Sie nicht an den Sandbox Analyzer übermitteln möchten.

Sie können auch Größenbeschränkungen für die übermittelten Objekte definieren, indem Sie das entsprechende Kontrollkästchen aktivieren und beliebige Werte zwischen 1 KB und 50 MB eingeben.

7. Unter **Detonationssprofil** können Sie den Komplexitätsgrad der Verhaltensanalyse festlegen. Dies hat Auswirkungen auf den Durchsatz des Sandbox Analyzers. Wenn Sie beispielsweise **Hoch** auswählen, führt der Sandbox Analyzer im gleichen Zeitraum eine genauere Analyse mit weniger Stichproben durch als bei **Mittel** oder **Gering**.

Der Sandbox Analyzer unterstützt die lokale Dateiübermittlung über Endpunkte mit Relais-Rolle, die Verbindungen zu verschiedenen Sandbox Analyzer-Portal-Adressen je nach Region herstellen können. Weitere Details zu den Relais-Konfigurationseinstellungen finden Sie hier: „Relais“ (S. 366).



Beachten Sie

Ein Proxy, der in den Verbindungseinstellungen des Sandbox Analyzer konfiguriert wurde, setzt sämtliche Endpunkte mit Relais-Rolle außer Kraft.

Netzwerksensor

In diesem Abschnitt können Sie die automatische Übermittlung von Stichproben aus dem Netzwerkdatenverkehr an Sandbox Analyzer über den Netzwerksensor konfigurieren. Dieses Modul erfordert, dass die Network Security Virtual Appliance mit Sandbox Analyzer On-Premises bereitgestellt und konfiguriert wird.

Gehen Sie folgendes vor, um die automatische Übermittlung per Netzwerksensor zu konfigurieren:

1. Markieren Sie das Kästchen **Automatische Stichproben-Übermittlung vom Netzwerksensor**, um die automatische Übermittlung von verdächtigen Dateien an den Sandbox Analyzer zu aktivieren.
2. Passen Sie unter **Vorabfilterung von Inhalten** die Sicherheitsstufe zur Abwehr potenzieller Bedrohungen an. Im Netzwerksensor ist ein Mechanismus zum Filtern von Inhalten eingebettet, der bestimmt, ob eine verdächtige Datei im Sandbox Analyzer detoniert werden muss.

Die folgenden Objekttypen werden unterstützt: Anwendungen, Dokumente, Skripte, Archive, E-Mails. Weitere Informationen zu den unterstützten Objekttypen finden Sie unter [„Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden“](#) (S. 550).

Über den Hauptschalter oben an der Bedrohungsliste können Sie eine einheitliche Sicherheitsstufe für alle Objekttypen festlegen, Sie können aber auch für jeden Typ eine eigene Stufe einstellen.

Wenn Sie das Modul auf eine bestimmte Stufe einstellen, führt dies zu einer bestimmten Anzahl von eingereichten Stichproben:

- **Tolerant.** Der Netzwerksensor übermittelt nur die Objekte automatisch an den Sandbox Analyzer, die am wahrscheinlichsten schädlich sind, und ignoriert alle übrigen Objekte.
- **Normal.** Der Netzwerksensor findet ein Gleichgewicht zwischen den übermittelten und ignorierten Objekten und übermittelt sowohl Objekte mit einer hohen und einer geringen Wahrscheinlichkeit, schädlich zu sein, an den Sandbox Analyzer.
- **Aggressiv.** Der Netzwerksensor übermittelt fast alle Objekte an den Sandbox Analyzer, unabhängig von ihrem potenziellen Risiko.

In einem eigenen Feld können Sie Ausnahmen für die Objekttypen festlegen, die Sie nicht an den Sandbox Analyzer übermitteln möchten.

Sie können auch Größenbeschränkungen für die übermittelten Objekte definieren, indem Sie das entsprechende Kontrollkästchen aktivieren und beliebige Werte zwischen 1 KB und 50 MB eingeben.

3. Wählen Sie unter **Verbindungseinstellungen** die bevorzugte Sandbox Analyzer-Instanz für die Übermittlung von Netzwerkinhalten aus.

Wenn sich Ihr Netzwerk hinter einem Proxy-Server oder einer Firewall befindet, können Sie das Kästchen **Proxy-Konfiguration verwenden** markieren und dann einen Proxy konfigurieren, um die Verbindung zum Sandbox Analyzer herzustellen.

Sie müssen die folgenden Felder ausfüllen:

- **Server** - die IP-Adresse des Proxy-Servers.
 - **Port** - der Port, über den die Verbindung zum Proxy-Server hergestellt wird.
 - **Benutzername** - ein Benutzername, der vom Proxy erkannt wird.
 - **Passwort** – das gültige Passwort für den entsprechenden Benutzer.
4. Unter **Detonationssprofil** können Sie den Komplexitätsgrad der Verhaltensanalyse festlegen. Dies hat Auswirkungen auf den Durchsatz des Sandbox Analyzers. Wenn Sie beispielsweise **Hoch** auswählen, führt der Sandbox Analyzer im gleichen Zeitraum eine genauere Analyse mit weniger Stichproben durch als bei **Mittel** oder **Gering**.

ICAP-Sensor

In diesem Abschnitt können Sie die automatische Übermittlung an den Sandbox Analyzer über den ICAP-Sensor konfigurieren.

Beachten Sie

Der Sandbox Analyzer benötigt einen Security Server, der zum Scannen von NAS-Geräten (Network Attached Storage) konfiguriert ist, die das ICAP-Protokoll verwenden. Weitere Einzelheiten dazu finden Sie unter „[Speicherschutz](#)“ (S. 406)

1. Markieren Sie das Kästchen **Automatische Stichproben-Übermittlung vom ICAP-Sensor**, um die automatische Übermittlung von verdächtigen Dateien an den Sandbox Analyzer zu aktivieren.
2. Passen Sie unter **Vorabfilterung von Inhalten** die Sicherheitsstufe zur Abwehr potenzieller Bedrohungen an. Im Netzwerksensor ist ein Mechanismus zum

Filtern von Inhalten eingebettet, der bestimmt, ob eine verdächtige Datei im Sandbox Analyzer detoniert werden muss.

Die folgenden Objekttypen werden unterstützt: Anwendungen, Dokumente, Skripte, Archive, E-Mails. Weitere Informationen zu den unterstützten Objekttypen finden Sie unter [„Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden“](#) (S. 550).

Über den Hauptschalter oben an der Bedrohungsliste können Sie eine einheitliche Sicherheitsstufe für alle Objekttypen festlegen, Sie können aber auch für jeden Typ eine eigene Stufe einstellen.

Wenn Sie das Modul auf eine bestimmte Stufe einstellen, führt dies zu einer bestimmten Anzahl von eingereichten Stichproben:

- **Tolerant.** Der ICAP-Sensor übermittelt nur die Objekte automatisch an den Sandbox Analyzer, die am wahrscheinlichsten schädlich sind, und ignoriert alle übrigen Objekte.
- **Normal.** Der ICAP-Sensor findet ein Gleichgewicht zwischen den übermittelten und ignorierten Objekten und übermittelt sowohl Objekte mit einer hohen und einer geringen Wahrscheinlichkeit, schädlich zu sein, an den Sandbox Analyzer.
- **Aggressiv.** Der ICAP-Sensor übermittelt fast alle Objekte an den Sandbox Analyzer, unabhängig von ihrem potenziellen Risiko.

In einem eigenen Feld können Sie Ausnahmen für die Objekttypen festlegen, die Sie nicht an den Sandbox Analyzer übermitteln möchten.

Sie können auch Größenbeschränkungen für die übermittelten Objekte definieren, indem Sie das entsprechende Kontrollkästchen aktivieren und beliebige Werte zwischen 1 KB und 50 MB eingeben.

3. Wählen Sie unter **Verbindungseinstellungen** die bevorzugte Sandbox Analyzer-Instanz für die Übermittlung von Netzwerkinhalten aus.

Wenn sich Ihr Netzwerk hinter einem Proxy-Server oder einer Firewall befindet, können Sie das Kästchen **Proxy-Konfiguration verwenden** markieren und dann einen Proxy konfigurieren, um die Verbindung zum Sandbox Analyzer herzustellen.

Sie müssen die folgenden Felder ausfüllen:

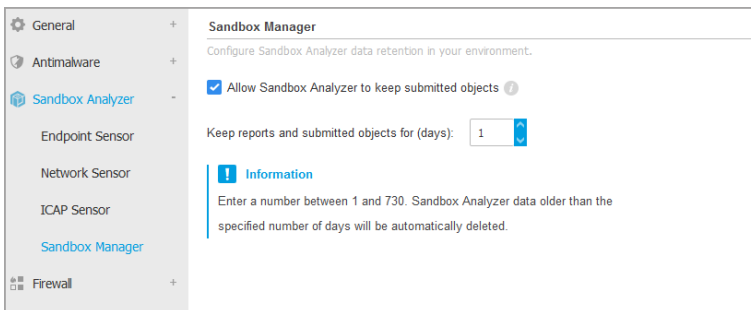
- **Server** - die IP-Adresse des Proxy-Servers.
- **Port** - der Port, über den die Verbindung zum Proxy-Server hergestellt wird.

- **Benutzername** - ein Benutzername, der vom Proxy erkannt wird.
 - **Passwort** – das gültige Passwort für den entsprechenden Benutzer.
4. Unter **Detonationssprofil** können Sie den Komplexitätsgrad der Verhaltensanalyse festlegen. Dies hat Auswirkungen auf den Durchsatz des Sandbox Analyzers. Wenn Sie beispielsweise **Hoch** auswählen, führt der Sandbox Analyzer im gleichen Zeitraum eine genauere Analyse mit weniger Stichproben durch als bei **Mittel** oder **Gering**.

Sandbox-Manager

In diesem Abschnitt konfigurieren Sie die Datenaufbewahrung für Ihre Sandbox Analyzer-Instanzen:

- Markieren Sie das Kästchen **Sandbox Analyzer erlauben, die übermittelten Objekte zu speichern**. Mit dieser Einstellung können Sie die Option **Erneut zur Analyse übermitteln** im Bereich der Übermittlungskarten der Sandbox Analyzer-Berichtsoberfläche verwenden.
- Geben Sie an, wie viele Tage Sandbox Analyzer Berichte und übermittelte Objekte im Datenspeicher speichern soll. Der Höchstwert ist 730. Nach Ablauf des festgelegten Zeitraums werden alle Daten gelöscht.



Richtlinien > Sandbox Analyzer > Sandbox Manager

7.2.5. Firewall



Beachten Sie

Dieses Modul steht für Windows for Workstations zur Verfügung.

Die Firewall schützt der Endpunkt vor nicht autorisierten Zugriffsversuchen bei eingehendem und ausgehendem Datentransfer.

Die Funktionsweise der Firewall basiert auf Netzwerkprofilen. Die Profile wiederum basieren auf Vertrauensstufen, die für jedes Netzwerk definiert werden müssen.

Die Firewall erkennt jede neue Verbindung, gleich die Informationen des Netzwerkadapters dieser Verbindung mit den Informationen der bestehenden Profile ab und wendet das entsprechende Profil an. Nähere Informationen zur Anwendung der Profile finden Sie unter „Netzwerkeinstellungen“ (S. 324).



Wichtig

Das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Allgemein
- Einstellungen
- Regeln

Allgemein

In diesem Bereich können Sie die Bitdefender-Firewall aktivieren und deaktivieren und die allgemeinen Einstellungen konfigurieren.

<ul style="list-style-type: none"> ⚙ Allgemein + 🛡 Malware-Schutz + 🔒 Firewall - <ul style="list-style-type: none"> Allgemein Einstellungen Regeln 📁 Inhalts-Steuer. + 🖨 Gerätesteuerung + ⌘ Relais + 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; padding: 5px 5px 0 5px;"> <input checked="" type="checkbox"/> Firewall </div> <div style="padding: 5px 5px 0 5px;"> <input checked="" type="checkbox"/> Port-Scans blockieren </div> <div style="padding: 5px 5px 0 5px;"> <input type="checkbox"/> Gemeinsame Nutzung der Internetverbindung (ICS) zulassen </div> <div style="padding: 5px 5px 0 5px;"> <input type="checkbox"/> WLAN-Verbindungen überwachen </div> <div style="padding: 5px 5px 0 5px;"> <input checked="" type="checkbox"/> Ausführlichkeitsstufe Protokoll Gering </div> <div style="padding: 5px 5px 0 5px;"> <input type="checkbox"/> Angriffserkennungssystem (IDS) </div> <div style="padding: 5px 5px 0 5px;"> <input type="radio"/> - Aggressiv Normal - für die meisten Systeme empfohlen </div> <div style="padding: 5px 5px 0 5px;"> <input checked="" type="radio"/> - Normal Schützt vor DLL-Injektionen und der Installation von Malware-Treibern. Schützt Bitdefender-Dateien vor Veränderungen durch nicht autorisierte Anwendungen. Gibt eine moderate Anzahl von Warnungen aus. </div> <div style="padding: 5px 5px 0 5px;"> <input type="radio"/> - Tolerant </div> </div>
---	---

Richtlinien für Computer und virtuelle Maschinen - Allgemeine Firewall-Einstellungen

- **Firewall.** Über das Kästchen können Sie die Firewall ein- oder ausschalten.



Warnung

Wenn Sie den Firewall-Schutz deaktivieren, werden die Computer anfällig für Angriffe über das Netzwerk und das Internet.

- **Port-Scans blockieren.** Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf einem Computer geöffnet sind. Wenn Sie dann einen unsicheren Port finden, können Sie in den Computer eindringen.
- **Gemeinsame Nutzung der Internetverbindung (ICS) zulassen.** Wählen Sie diese Option, damit die Firewall die gemeinsame Nutzung der Internetverbindung zulässt.



Beachten Sie

Diese Option aktiviert nicht automatisch die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing) auf dem Computer des Benutzers.

- **WLAN-Verbindungen überwachen.** Der Bitdefender-Sicherheitsagent kann Benutzer in einem Drahtlosnetzwerk über neu zum Netzwerk hinzugekommene Computer informieren. Wählen Sie diese Option aus, um solche Benachrichtigungen auf dem Bildschirm des Benutzers anzuzeigen.
- **Ausführlichkeitsstufe Protokoll.** Der Bitdefender-Sicherheitsagent erstellt ein Protokoll der Ereignisse, die im Zusammenhang mit der Nutzung des Firewall-Moduls auftreten (Aktivieren/Deaktivieren der Firewall, Blockieren des Datenverkehrs, Einstellungsänderungen) oder die durch Aktivitäten erzeugt wurden, die von diesem Modul erkannt wurden (Port-Scans, regelbasiertes Blockieren von Verbindungsversuchen und Datenverkehr). Wählen Sie unter **Ausführlichkeitsstufe Protokoll** eine Option aus, um festzulegen, wie viele Informationen im Protokoll enthalten sein sollen.
- **Angriffserkennungssystem (IDS).** Das Angriffserkennungssystem (IDS) überwacht das System und sucht nach verdächtigen Aktivitäten (so zum Beispiel unerlaubte Versuche, Bitdefender-Dateien zu verändern, DLLs einzuschleusen, Tastaturanschläge zu protokollieren, etc.).



Beachten Sie

Die Richtlinieneinstellungen für das Angriffserkennungssystem (IDS) gelten nur für Endpoint Security (alter Sicherheitsagent). Im Bitdefender Endpoint Security Tools-Agent sind die Host-basierten Funktionen des Angriffserkennungssystems im Modul Advanced Threat Control (ATC) integriert.

Um das Angriffserkennungssystem (IDS) zu konfigurieren:

1. Über das Kästchen können Sie das Angriffserkennungssystem (IDS) ein- oder ausschalten.
2. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Um zu verhindern, dass eine harmlose Anwendung vom Angriffserkennungssystem erkannt wird, fügen Sie eine **ATC/IDS-Prozessausschlussregel** für diese Anwendung im Bereich **Malware-Schutz > Einstellungen > Benutzerdefinierte Ausschlüsse** hinzu.



Wichtig

Das Angriffserkennungssystem ist nur für Endpoint Security-Clients verfügbar.

Einstellungen

Je nach Vertrauensstufe wendet die Firewall automatisch ein Profil an. Verschiedene Netzwerkverbindungen können unterschiedliche Vertrauensstufen haben, je nach Architektur des Netzwerk oder Art des Adapters, über den die Verbindung hergestellt wird. Wenn Sie zum Beispiel Subnetzwerke in Ihrem Unternehmensnetzwerk haben, können Sie für jedes Subnetzwerk eine eigene Vertrauensstufe festlegen.

Die Einstellungen sind in den folgenden Tabellen sortiert:

- [Netzwerke](#)
- [Adapter](#)

- ⚙ Allgemein +
- 🛡 Malware-Schutz +
- 🔒 Firewall +
- Allgemein
- Einstellungen
- Regeln
- ⚙ Inhalts-Steuer. +
- 🔧 Gerätesteuerung +
- ⋮ Relais +

Netzwerke ⓘ

Name	Typ ⓘ	Identifikation	MAC	IP ⓘ	Aktion

Adapter ⓘ

Typ	Netzwerktyp ⓘ	Netzwerk-Unsichtbarkeit ⓘ
Wired	Heim/Büro	Aus
Wireless (Kabellos)	Öffentlich	Aus

Richtlinien - Firewall Einstellungen

Netzwerkeinstellungen

Wenn Sie möchten, dass die Firewall verschiedenen Bereichen Ihres Unternehmens unterschiedliche Profile zuweist, müssen Sie die verwalteten Netzwerke in der Tabelle **Netzwerke** angeben. Füllen Sie die Felder der Tabelle **Netzwerke** wie folgt aus:

- **Name.** Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- **Typ.** Hier können Sie aus dem Menü die Art des Profils wählen, das dem Netzwerk zugewiesen wird.

Der Bitdefender-Sicherheitsagent wendet automatisch eins der vier Netzwerk-Profile auf jede erkannte Netzwerkverbindung des Endpunkts an, um die grundlegenden Datenverkehrfiltermöglichkeiten festzulegen. Es gibt folgende Profiltypen:

- **Vertrauenswürdiges Netzwerk.** Deaktiviert die Firewall für die entsprechenden Adapter.
- **Heim-/Büronetzwerk.** Lässt sämtlichen Datenverkehr zwischen den Computern im lokalen Netzwerk zu; anderer Datenverkehr wird gefiltert.
- **Öffentliches Netzwerk.** Sämtlicher Datenverkehr wird gefiltert.
- **Nicht vertrauenswürdiges Netzwerk.** Der Netzwerk- und Internet-Datenverkehr über die entsprechenden Adapter wird vollständig blockiert.
- **Identifikation.** Wählen Sie aus dem Menü die Methode, nach der der Bitdefender-Sicherheitsagent ein Netzwerk identifiziert. Es gibt drei Methoden zur Identifizierung: **DNS**, **Gateway** und **Netzwerk**.
 - **DNS:** identifiziert alle Endpunkte über das angegebene DNS.
 - **Gateway:** identifiziert alle Endpunkte, die über das angegebene Gateway kommunizieren.
 - **Netzwerk:** identifiziert alle Endpunkte aus dem angegebenen Netzwerkbereich nach der entsprechenden Netzwerkadresse.
- **MAC.** In diesem Feld können Sie die MAC-Adresse eines DNS-Servers oder eines Gateways des Netzwerks angeben, je nach ausgewählter Identifikationsmethode. Die MAC-Adresse müssen Sie im Hexadezimalformat eingeben, durch Bindestriche (-) oder Doppelpunkte (:) getrennt. So sind z. B. sowohl 00-50-56-84-32-2b als auch 00:50:56:84:32:2b gültige Adressen.

- **IP.** In diesem Feld können Sie bestimmte IP-Adressen in einem Netzwerk definieren. Das Format der IP-Adresse hängt wie folgt von der Identifikationsmethode ab:
 - **Netzwerk.** Geben Sie die Netzwerknummer im CIDR-Format ein. Zum Beispiel `192.168.1.0/24`, wobei `192.168.1.0` die Netzwerkadresse ist und `/24` die Netzwerkmaske.
 - **Gateway.** Geben Sie die IP-Adresse des Gateways ein.
 - **DNS.** Geben Sie die IP-Adresse des DNS-Servers ein.

Nachdem Sie ein Netzwerk definiert haben, klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle, um das Netzwerk der Liste hinzuzufügen.

Adaptoreinstellungen

Wenn ein Netzwerk erkannt wird, das nicht in der Tabelle **Netzwerke** definiert ist, erkennt der Bitdefender-Sicherheitsagent die Art des Netzwerkadapters und wendet ein passendes Profil auf die Netzwerkverbindung an.

Die Felder der Tabelle **Adapter** werden folgend beschrieben:

- **Typ.** Zeigt die Art des Netzwerkadapters an. Der Bitdefender-Sicherheitsagent kann drei verschiedene vordefinierte Adaptertypen erkennen: **Kabelgebunden**, **Kabellos** und **Virtuell** (Virtuelles Privates Netzwerk).
- **Netzwerktyp.** Beschreibt das Netzwerkprofil, das einem bestimmten Adaptertyp zugewiesen ist. Die Netzwerkprofile sind im Abschnitt [Netzwerkeinstellungen](#) beschrieben. Wenn Sie auf das Netzwerktypfeld klicken, können Sie die Einstellung ändern.

Wenn Sie **Windows entscheiden lassen** wählen, wendet der Bitdefender-Sicherheitsagent für jede neue Netzwerkverbindung, die erkannt wird, nachdem die Richtlinie angewendet wurde, ein Profil für die Firewall an, das auf der Netzwerkklassifikation in Windows basiert. Die Einstellungen der Tabelle **Adapter** werden dabei ignoriert.

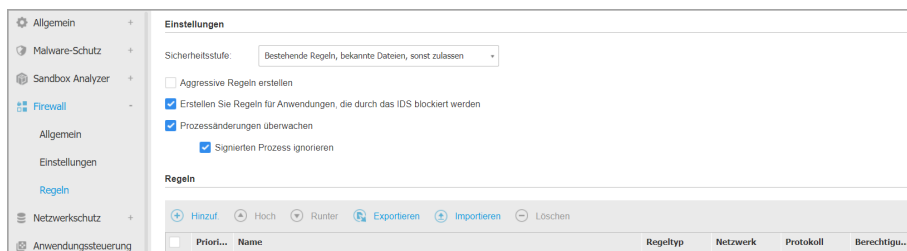
Wenn die Erkennung auf der Basis des Windows-Netzwerkmanagers fehlschlägt, wird eine einfache Erkennung versucht. Ein generisches Profil wird angewendet, in dem das Netzwerkprofil **Öffentlich** zugrundegelegt und die Tarnkappeneinstellung auf **Ein** gestellt wird.

Wenn der in Active Directory eingebundene Endpunkt eine Verbindung mit der Domain herstellt, wird das Firewall-Profil automatisch auf **Heim/Büro** und die Tarnkappeneinstellungen auf **Remote** gesetzt. Wenn der Computer nicht in einer Domain ist, wird diese Bedingung ignoriert.

- **Netzwerkerkennung.** Macht Ihren Computer im Netzwerk oder Internet unsichtbar für schädliche Software und Hacker. Konfigurieren Sie die Sichtbarkeit des Computers im Netzwerk nach Bedarf für jeden Adaptertypen, indem Sie jeweils eine der folgenden Optionen auswählen:
 - **Ja.** Jeder Benutzer in lokalen Netzwerk oder dem Internet kann den Computer anpingen oder finden.
 - **Nein.** Der Computer kann weder über das lokale Netzwerk noch über das Internet gefunden werden.
 - **Remote.** Der Computer kann nicht über das Internet erkannt werden. Jeder Benutzer im lokalen Netzwerk kann den Computer anpingen oder erkennen.

Regeln

In diesem Bereich können Sie den Netzwerkzugriff für Anwendungen und die Firewall-Regeln für den Datenverkehr festlegen. Bitte beachten Sie, dass die verfügbaren Einstellungen nur auf die **Heim/Büro-** oder **Öffentlichen Profile** angewendet werden können.



Richtlinien für Computer und virtuelle Maschinen - Firewall-Regeleinstellungen

Einstellungen

Sie können die folgenden Einstellungen vornehmen:

- **Sicherheitsstufe.** Die ausgewählte Sicherheitsstufe definiert die Firewall-Entscheidungslogik, die verwendet wird, wenn Anwendungen den Zugriff

auf Netzwerk- oder Internet-Dienste anfordern. Die folgenden Optionen stehen zur Verfügung:

Bestehende Regeln, sonst zulassen

Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch zulassen. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln und nachfragen

Bestehende Firewall-Regeln anwenden und den Benutzer für alle weiteren Verbindungsversuche zur Auswahl einer Aktion auffordern. Ein Warnfenster mit detaillierten Informationen über den unbekanntem Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, sonst verweigern

Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch verweigern. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst zulassen

Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren unbekanntem Verbindungsversuche automatisch zulassen. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien und nachfragen

Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und den Benutzer für alle weiteren unbekanntem Verbindungsversuche zur Auswahl einer Aktion auffordern. Ein Warnfenster mit detaillierten Informationen über den unbekanntem Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst verweigern

Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren

unbekannten Verbindungsversuche automatisch verweigern. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.



Beachten Sie

Bekannte Dateien sind eine Sammlung von sicheren und vertrauenswürdigen Anwendungen, die von Bitdefender zusammengestellt und fortlaufend gepflegt wird.

- **Aggressive Regeln erstellen.** Wenn diese Option aktiviert ist, werden für jeden Prozess, der die Anwendung öffnet, die Zugriff auf das Netzwerk oder das Internet anfordert, von der Firewall Regeln erstellt.
- **Erstellen Sie Regeln für Anwendungen, die durch das IDS blockiert werden.** Wenn diese Option ausgewählt ist, erstellt die Firewall jedes Mal, wenn das Angriffserkennungssystem eine Anwendung blockiert, automatisch eine **Verweigern**-Regel.
- **Prozessänderungen überwachen.** Wählen Sie diese Option, wenn Sie möchten, dass jede Anwendung, die sich mit dem Internet verbinden möchte, darauf überprüft wird, ob sie seit der Festlegung der Regel für ihren Internetzugriff verändert wurde. Falls die Anwendung geändert wurde, wird eine neue Regel in Übereinstimmung mit dem aktuellen Sicherheitsstufe angelegt.



Beachten Sie

Normalerweise werden Anwendungen durch Updates verändert. Es kann aber auch sein, dass eine Anwendung durch Malware verändert wird um den lokalen Computer oder andere Computer in dem Netzwerk zu infizieren.

Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad. Wählen Sie **Signierten Prozess ignorieren**, um veränderten signierten Anwendungen automatisch die Verbindung mit dem Internet zu erlauben.

Regeln

In der Regeltabelle werden die aktuellen Firewall-Regeln mit wichtigen Informationen zu den einzelnen Regel angezeigt:

- Name der Regel oder Anwendung, auf die sie sich bezieht.
- Protokoll, auf das die Regel angewendet werden soll.

- Aktion der Regel (Pakete zulassen oder verweigern).
- Für die Regel verfügbare Aktionen.
- Regelpriorität.



Beachten Sie

Diese Firewall-Regeln werden ausdrücklich von der Richtlinie umgesetzt. Zusätzliche Regeln werden unter Umständen auf Computern als Folge der Anwendung von Firewall-Einstellungen konfiguriert.

Eine Reihe von Standardregeln für die Firewall helfen Ihnen dabei, häufig genutzte Datenverkehrstypen ohne viel Aufwand zuzulassen oder zu verweigern. Wählen Sie die gewünschte Option aus dem **Berechtigung**-Menü.

Eingehende ICMP / ICMPv6

ICMP- / ICMPv6-Nachrichten zulassen oder verweigern. ICMP-Nachrichten werden häufig von Hackern für Angriffe auf Computer-Netzwerke genutzt. Standardmäßig wird diese Art Datenverkehr zugelassen.

Eingehende Remote-Desktop-Verbindungen

Den Zugriff anderer Computer über Remote-Desktop-Verbindungen zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

E-Mails versenden

Versand von E-Mails über SMTP zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

Web-Browsing HTTP

HTTP-Browsing zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

Drucken übers Netzwerk

Den Zugriff auf Drucker in anderen lokalen Netzwerken erlauben oder verweigern. Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Windows-Explorer-Datenverkehr auf HTTP / FTP

HTTP- und FTP-Datenverkehr aus Windows Explorer heraus zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Neben den Standardregeln können Sie weitere Firewall-Regeln für andere auf den Endpunkten installierte Anwendungen erstellen. Diese Konfiguration bleibt jedoch Administratoren vorbehalten, die über umfangreiche Netzwerkkennnisse verfügen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche **+** **Hinzufügen** am rechten Rand der Tabelle. Weitere Informationen finden Sie [hier](#).

Um eine Regel aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche **-** **Löschen** am oberen Rand der Tabelle.



Beachten Sie

Sie können die Standard-Firewall-Regeln weder löschen noch bearbeiten.

Benutzerdefinierte Regeln konfigurieren

Sie können zwei Arten von Firewall-Regeln konfigurieren:

- **Anwendungsbasierte Regeln.** Diese Regeln gelten für bestimmte Programme auf den Client-Computern.
- **Verbindungsbasierte Regeln.** Diese Regeln gelten für alle Anwendungen oder Dienste, die eine bestimmte Verbindung nutzen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche **+** **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie den gewünschten Regeltyp aus dem Menü. Um eine bestehende Regel zu bearbeiten, klicken Sie auf den Namen der Regel.

Die folgenden Einstellungen können konfiguriert werden:

- **Name der Regel.** Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll (so zum Beispiel den Namen der Anwendung, auf die die Regel angewendet wird).
- **Anwendungspfad** (nur für anwendungsbasierte Regeln). Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben.
 - Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad nach Bedarf. So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%ProgramFiles%` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
 - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

- **Befehlszeile** (nur für anwendungsbasierte Regeln). Wenn die Regel nur angewendet werden soll, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Windows-Befehlszeile geöffnet wird, geben Sie den entsprechenden Befehl in das Bearbeitungsfeld ein. Andernfalls lassen Sie das Feld frei.
- **Anwendungs-MD5** (nur für anwendungsbasierte Regeln). Wenn die Regel die Integrität der Dateidaten der Anwendung anhand des MD5-Hashcodes überprüfen soll, geben Sie ihn in das Bearbeitungsfeld ein. Lassen Sie das Feld ansonsten frei.
- **Lokale Adresse**. Geben Sie die lokale IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Wenn Sie mehr als einen Netzwerkadapter haben, können Sie die Markierung im Kästchen **Alle** aufheben und eine bestimmte IP-Adresse eingeben. Um Verbindungen über einen bestimmten Port oder Port-Bereich zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie den gewünschten Port oder Port-Bereich in das entsprechende Feld ein.
- **Remote-Adresse**. Geben Sie die Remote-IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Um den ein- und ausgehenden Datenverkehr auf einem bestimmten Computer zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie seine IP-Adresse ein.
- **Regel nur für direkt verbundene Computer anwenden**. Sie können den Zugriff anhand der MAC-Adresse filtern.
- **Protokoll**. Wählen Sie das IP-Protokoll, auf das die Regel angewendet werden soll.
 - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
 - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
 - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
 - Wenn die Regeln für ein bestimmtes Protokoll gelten soll, wählen Sie das gewünschte Protokoll aus dem Menü **Sonstige**.



Beachten Sie

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. Die komplette Liste zugewiesener Nummern

von IP-Protokollen finden Sie unter <http://www.iana.org/assignments/protocol-numbers>.

- **Richtung.** Wählen Sie die Datenverkehrsrichtung an, auf die die Regel angewendet werden soll.

Richtung	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf den ausgehenden Datenverkehr.
Eingehend	Die Regel bezieht sich nur auf den eingehenden Datenverkehr.
Beides	Die Regel findet in beiden Richtungen Anwendung.

- **IP-Version.** Wählen Sie die IP-Version (IPv4, IPv6 oder andere), auf die die Regel angewendet werden soll.
- **Netzwerk.** Wählen Sie den Netzwerktyp aus, auf den die Regel angewendet werden soll.
- **Berechtigung.** Wählen Sie eine der verfügbaren Berechtigungs-Optionen:

Berechtigung	Beschreibung
JA	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

Ordnen Sie die Regeln, die Sie erstellt haben, mithilfe der Pfeile auf der rechten Seite der Tabelle nach ihrer Priorität. Je weiter oben eine Regel in der Liste steht, desto höher ist ihre Priorität.

Regeln importieren und exportieren

Sie können Firewall-Regeln importieren und exportieren, um sie in anderen Richtlinien und/oder Unternehmen zu verwenden. So exportieren Sie Regeln:

1. Klicken Sie dazu oben an der Regeltabelle auf **Exportieren**.

2. Speichern Sie die CSV-Datei auf Ihrem Computer. Je nach den Browser-Einstellungen wird die Datei automatisch heruntergeladen oder Sie werden aufgefordert, einen Speicherort für sie zu wählen.

Wichtig

- Jede Zeile in der CSV-Datei entspricht einer einzelnen Regel und hat mehrere Felder:
- Die Priorität der Firewall-Regeln wird durch ihre Position in der CSV-Datei vorgegeben. Sie können die Priorität einer Regel verändern, indem Sie die gesamte Zeile verschieben.

Bei den Standardregeln können Sie nur die folgenden Elemente verändern:

- **Priorität:** Sie können die Priorität der Regeln beliebig verändern, indem Sie die Zeilen innerhalb der CSV-Datei verschieben.
- **Berechtigung:** Im Feld `set.Permission` können Sie die folgenden Einstellungen wählen.
 - 1 für **Zulassen**
 - 2 für **Verweigern**

Andere Werte werden beim Import ignoriert.

Für benutzerdefinierte Firewall-Regeln können die Felder wie folgt konfiguriert werden:

Feld	Name und Wert
<code>ruleType</code>	Regeltyp: 1 für Anwendungsregel 2 für Verbindungsregel
<code>Art</code>	Der Wert für dieses Feld ist optional.
<code>details.name</code>	Name der Regel
<code>details.applictionPath</code>	Anwendungspfad (nur für anwendungsbasierte Regeln)
<code>details.commandLine</code>	Befehlszeile (nur für anwendungsbasierte Regeln)



Feld	Name und Wert
details.applicationMd5	Anwendungs-MD5 (nur für anwendungsbasierte Regeln)
settings.protocol	Protokoll 1 für Alle 2 für TCP 3 für UDP 4 für Andere
settings.customProtocol	Nur erforderlich, wenn bei Protokoll Andere eingestellt ist. Details zu den einzelnen Werten finden Sie auf dieser Seite . Die Werte 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 werden nicht unterstützt.
settings.direction	Richtung: 1 für Beide 2 für Eingehend 3 für Ausgehend
settings.ipVersion	IP-Version: 1 für Alle 2 für IPv4 3 für IPv6
settings.localAddress.any	Bei Lokale Adresse ist Alle eingestellt: 1 für Wahr 0 oder leer lassen für Falsch
settings.localAddress.ipMask	Bei Lokale Adresse ist IP oder IP/Maske eingestellt
settings.remoteAddress.portRange	Bei Remote-Adresse ist Port oder Port-Bereich eingestellt



Feld	Name und Wert
settings.directlyConnected.enable	Regel nur für direkt verbundene Computer anwenden: 1 für Aktiviert 0 oder leer lassen für Deaktiviert
settings.directlyConnected.remoteMac	Regel nur für direkt verbundene Computer anwenden mit MAC-Adresse-Filter.
permission.home	Das Netzwerk , für das die Regel gilt, ist Heim/Büro : 1 für Wahr 0 oder leer lassen für Falsch
permission.public	Das Netzwerk , für das die Regel gilt, ist Öffentlich : 1 für Wahr 0 oder leer lassen für Falsch
permission.setPermission	Verfügbare Berechtigungen: 1 für Zulassen 2 für Verweigern

So importieren Sie Regeln:

1. Klicken Sie dazu oben an der Regeltabelle auf **Importieren**.
2. Klicken Sie im neuen Fenster auf **Hinzufügen** und wählen Sie die CSV-Datei.
3. Klicken Sie auf **Speichern**. Die Tabelle wird mit den gültigen Regeln gefüllt.

7.2.6. Netzwerkschutz

Im Abschnitt Netzwerkschutz können Sie Ihre Einstellungen für die Inhaltsfilterung, den Identitätsschutz für Benutzeraktivitäten wie Webbrowsing, E-Mail- und Softwareanwendungen sowie die Erkennung von Netzwerkangriffstechniken konfigurieren, die versuchen, auf bestimmte Endpunkte zuzugreifen. Sie können den Zugriff auf das Internet und bestimmte Anwendungen einschränken und Datenverkehr-Scans, Phishing-Schutz- und Identitätsschutzregeln konfigurieren.

Bitte beachten Sie, dass die Einstellungen für den Netzwerkschutz auf alle Benutzer angewendet werden, die sich an den Ziel-Computern anmelden.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [Allgemein](#)
- [Inhalts-Steuerung](#)
- [Internet-Schutz](#)
- [Netzwerkangriffe](#)

Beachten Sie

- Das Inhaltssteuerungsmodul ist verfügbar für:
 - Windows für Workstations
 - macOS
- Das Network Attack Defense-Modul ist verfügbar für:
 - Windows für Workstations

Wichtig

Unter macOS ist für die Inhaltssteuerung eine Kernel-Erweiterung erforderlich. Die Installation einer Kernel-Erweiterung erfordert unter macOS High Sierra (10.13) und höher Ihre Zustimmung. Das System benachrichtigt den Benutzer, dass eine Bitdefender-Systemerweiterung blockiert wurde. Der Benutzer kann die Zustimmung dazu in den Einstellungen unter **Sicherheit & Datenschutz** erteilen. Dieses Modul funktioniert erst, wenn der Benutzer der Bitdefender-Systemerweiterung zugestimmt hat. Bis dahin wird in der Endpoint Security for Mac-Benutzeroberfläche ein kritisches Problem angezeigt und die Zustimmung angefordert.

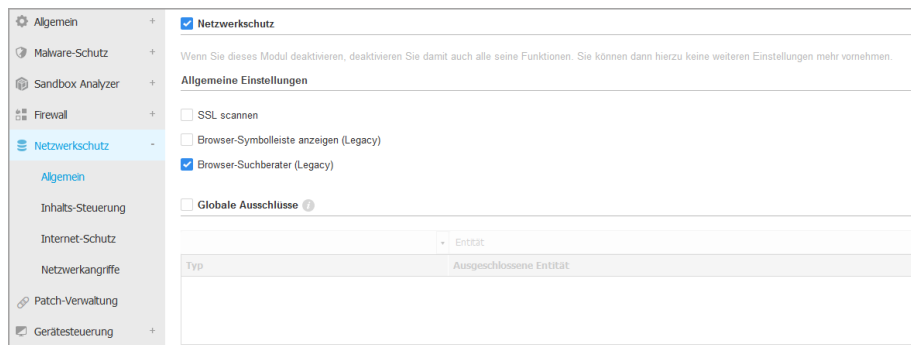
Um den Benutzern Aufwand zu ersparen, kann die Bitdefender-Kernelerweiterung auch im Voraus genehmigt werden, indem sie mithilfe eines Mobilgerät-Verwaltungstools auf die Whitelist gesetzt wird. Weitere Details zu Bitdefender-Kernelerweiterungen finden Sie in [diesem Artikel](#).

Allgemein

Auf dieser Seite können Sie Optionen wie das Aktivieren oder Deaktivieren von Funktionalitäten sowie Ausschlüsse konfigurieren.


Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [Allgemeine Einstellungen](#)
- [Globale Ausschlüsse](#)



Richtlinien für Computer und virtuelle Maschinen - Netzwerkschutz - Allgemein

Allgemeine Einstellungen

- **SSL scannen.** Wählen Sie diese Option, wenn der SSL-Datenverkehr (Secure Sockets Layer) von den Sicherheitsmodulen des Bitdefender-Sicherheitsagenten überprüft werden soll.
- **Browser-Symboleiste anzeigen (Legacy).** Die Bitdefender-Symboleiste informiert Benutzer über die Bewertung der Webseiten, die sie aufrufen. Die Bitdefender-Symboleiste ist anders als andere Browser-Symboleisten. Sie fügt lediglich einen kleinen Dragger  zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symboleiste.

Abhängig davon, wie Bitdefender die Webseite einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symboleiste eingeblendet:

- Die Nachricht "Diese Website ist nicht sicher" erscheint auf rotem Hintergrund.
- Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund.
- Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund.



Beachten Sie

- Diese Option ist unter macOS nicht verfügbar.
- Diese Option ist unter Windows bei Neuinstallationen von Bitdefender Endpoint Security Tools ab Version 6.6.5.82 nicht mehr enthalten.

- **Browser-Suchberater (Legacy).** Der Suchberater bewertet sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis platziert. Verwendete Symbole und ihre Bedeutung:
 - ✖ Sie sollten diese Webseite nicht aufrufen.
 - ⚠ Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.
 - ✔ Diese Seite ist sicher.



Beachten Sie

- Diese Option ist unter macOS nicht verfügbar.
- Diese Option ist unter Windows bei Neuinstallationen von Bitdefender Endpoint Security Tools ab Version 6.6.5.82 nicht mehr enthalten.

Globale Ausschlüsse

Wenn die **Netzwerkschutz**-Optionen aktiviert sind, können Sie bestimmte Arten von Datenverkehr vom Scan auf Malware ausschließen.



Beachten Sie

Diese Ausschlüsse gelten für **Datenverkehr-Scan** und **Phishing-Schutz** im Bereich **Internet-Schutz** und für **Network Attack Defense** im Bereich **Netzwerkangriffe**. Ausschlüsse für den **Identitätsschutz** können separat im Bereich **Inhaltssteuerung** konfiguriert werden.

So können Sie Ausschlüsse definieren:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. So definieren Sie je nach Ausschlusstyp die Datenverkehrsentität, die vom Scan ausgeschlossen werden soll:
 - **IP-Adresse/Maske.** Geben Sie die IP-Adresse oder die IP-Maske ein, für die der ein- und ausgehende Datenverkehr (das schließt auch Netzwerkangriffstechniken ein) nicht gescannt werden soll
 - **URL.** Schließt die eingegebenen Web-Adressen vom Scan aus. Beachten Sie, dass es zwischen HTTP- und HTTPS-Verbindungen Unterschiede bei der Anwendung von URL-basierten Scan-Ausschlüssen gibt. Diese werden im Folgenden erläutert.

Sie können einen URL-basierten Scan-Ausschluss wie folgt definieren:

- Geben Sie eine bestimmte URL ein, z. B. `www.example.com/example.html`
 - Bei HTTP-Verbindungen wird nur die konkrete URL vom Scan ausgeschlossen.
 - Bei HTTPS-Verbindungen werden durch das Hinzufügen einer bestimmten URL die gesamte Domäne und alle Subdomänen ausgeschlossen. Darum können Sie in diesem Fall direkt die Domäne angeben, die vom Scan ausgeschlossen werden soll.
- Verwenden Sie Platzhalter, um Webadressmuster zu definieren (nur bei HTTP-Verbindungen).



Wichtig

Platzhalterausschlüsse funktionieren bei HTTPS-Verbindungen.

Sie können die folgenden Platzhalter verwenden:

- Ein Sternchen (*) ersetzt null oder mehr Zeichen.
- Ein Fragezeichen (?) ersetzt genau ein Zeichen. Sie können mehrere Fragezeichen benutzen, um eine beliebige Kombination einer bestimmten Anzahl von Zeichen zu ersetzen. Drei Fragezeichen ??? ersetzen zum Beispiel jede beliebige Kombination aus genau 3 Zeichen.

In der folgenden Tabelle finden Sie eine Reihe von Syntaxbeispielen für die Angabe von Webadressen (URL).

Syntax	Anwendungsbereich des Ausschlusses
<code>www.beispiel*</code>	Eine beliebige URL, die mit <code>www.Beispiel</code> beginnt (unabhängig von der Domainendung). Der Ausschluss gilt nicht für die Unterdomänen der angegebenen Website, so zum Beispiel <code>unterdomäne.beispiel.com</code> .
<code>*beispiel.com</code>	Jede URL, die mit <code>Beispiel.com</code> aufhört, einschließlich aller Subdomains.

Syntax	Anwendungsbereich des Ausschlusses
beispiel.com	Alle URLs, die die angegebene Zeichenfolge enthalten.
*.com	Jede Website mit der Domainendung .com, einschließlich aller Subdomains. Mit dieser Syntax können Sie eine gesamte Top-Level-Domain vom Scan ausschließen.
www.beispiel?.com	Jede Internet-Adresse, die mit www.beispiel?.com beginnt. Das Fragezeichen kann dabei für jedes beliebige einzelne Zeichen stehen. Beispiele hierfür sind www.beispiel1.com oder www.beispielA.com.



Beachten Sie

Sie können relative URLs verwenden.

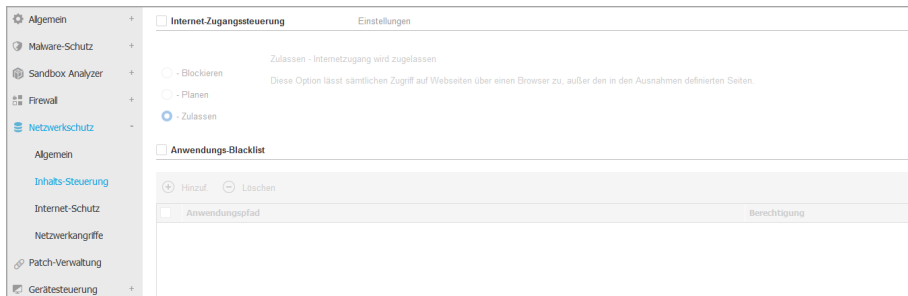
- **Anwendung.** Schließt den angegebenen Prozess oder die Anwendung vom Scan aus. So definieren Sie einen Anwendungs-Scan-Ausschluss:
 - Geben Sie den vollständigen Anwendungspfad ein. Zum Beispiel `C:\Programme\Internet Explorer\iexplore.exe`
 - Sie können auch Umgebungsvariablen verwenden, um den Anwendungspfad anzugeben. Zum Beispiel: `%programfiles%\Internet Explorer\iexplore.exe`
 - Oder Sie verwenden Platzhalter, um alle Anwendungen zusammenzufassen, die einem bestimmten Muster folgen. Zum Beispiel:
 - `c*.exe` erfasst alle Anwendungen, die mit "c" beginnen (z. B. `chrome.exe`).
 - `??????.exe` umfasst alle Anwendungen, deren Name genau sechs Zeichen lang ist (`chrome.exe`, `safari.exe`, usw.).
 - `[^c]*.exe` umfasst alle Anwendungen, außer denen, die mit "c" beginnen.
 - `[^ci]*.exe` umfasst alle Anwendungen immer außer denen, die mit "c" oder "i" beginnen.

3. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle. Um eine Entität aus der Liste zu löschen, klicken Sie auf die entsprechende **⊗ Löschen**-Schaltfläche.

Inhalts-Steuerung

Die Einstellungen für die Inhaltssteuerung sind in die folgenden Bereiche eingeteilt:

- **Internet-Zugangssteuerung**
- **Anwendungs-Blacklist**
- **Datenschutz**



Internet-Zugangssteuerung

Mit der Internet-Zugangssteuerung können Sie den Internet-Zugang für Benutzer oder Anwendungen für bestimmte Zeiträume zulassen oder blockieren.

Die Webseiten die von der Internet-Zugangssteuerung blockiert werden, werden nicht im Browser angezeigt. Stattdessen wird eine Standardseite angezeigt, die den Nutzer darüber informiert, dass die angeforderte Webseite von der Internet-Zugangssteuerung blockiert wurde.

Mit dem Schalter können Sie die **Internet-Zugangssteuerung** ein- und ausschalten. Sie haben drei Konfigurationsoptionen:

- Mit **Zulassen** lassen Sie den Internetzugriff immer zu.
- Mit **Blockieren** lassen Sie den Internetzugriff nie zu.
- Mit **Planen** können Sie einen Zeitplan für den Internetzugriff festlegen.

Wenn Sie den Internetzugriff zulassen oder blockieren, können Sie Ausnahmen zu diesen Einstellungen definieren; für ganze Internetkategorien oder für bestimmte einzelne Internetadressen. Klicken Sie auf **Einstellungen** und konfigurieren Sie den Zeitplan bzw. die Ausnahmen wie folgt:

Planer

So schränken Sie den Internet-Zugang auf bestimmte Tageszeiten während der Woche ein:

1. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert werden soll.

Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.

Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.

2. Klicken Sie auf **Speichern**.



Beachten Sie

Der Bitdefender-Sicherheitsagent führt unabhängig davon, ob der Internetzugang gesperrt ist, stündlich Updates durch.

Kategorien

Internetkategorienfilter filtern den Zugriff auf Websites dynamisch anhand derer Inhalte. Sie können den Internetkategorienfilter verwenden, um Ausnahmen zur gewählten Aktion (Zulassen oder Blockieren) für ganze Kategorien (z. B. Spiele, nicht jugendfreies Material oder Online-Netzwerke) zu definieren.

So konfigurieren Sie die Internetkategorienfilter:

1. Aktivieren Sie **Internet-Kategorienfilter**.
2. Für eine schnelle Konfiguration können Sie auf eines der vordefinierten Profile (**aggressiv**, **normal**, **tolerant**) klicken. Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala. Wenn Sie den Bereich **Internet-Regeln** unten erweitern, können Sie die vordefinierten Aktionen für bestehende Internetkategorien anzeigen.
3. Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie einen benutzerdefinierten Filter anlegen:

- a. Wählen Sie **Benutzerdefiniert**.
 - b. Klicken Sie auf **Internet-Regeln**, um den entsprechenden Bereich zu erweitern.
 - c. Suchen Sie die gewünschte Kategorie in der Liste und wählen Sie die gewünschte Aktion aus dem Menü. Weitere Informationen zu den verfügbaren Website-Kategorien finden Sie in [diesem Artikel](#).
4. Sie können auch **Internetkategorien als Ausnahmen für den Internetzugriff behandeln**, wenn Sie die bestehenden Internetzugriffseinstellungen ignorieren und nur den Internetkategorienfilter benutzen möchten.
 5. In der Standardnachricht an einen Benutzer, der eine unerwünschte Website aufgerufen hat, wird auch die Kategorie erwähnt, aufgrund derer die Website blockiert wurde. Deaktivieren Sie die Option **Detaillierte Warnungen auf dem Client anzeigen**, wenn Sie diese Informationen vor den Benutzern verbergen möchten.

**Beachten Sie**

Diese Option ist unter macOS nicht verfügbar.

6. Klicken Sie auf **Speichern**.

**Beachten Sie**

- Bestimmte Internetadressen, für die die Berechtigung **Zulassen** eingestellt ist, werden während der Zeiten, zu denen der Internetzugang durch die Internet-Zugangssteuerung blockiert ist, berücksichtigt.
- Das **Zulassen** funktioniert nur, wenn der Internet-Zugang durch die Internet-Zugangssteuerung blockiert ist. Das **Blockieren** funktioniert nur, wenn der Internet-Zugang über die Internet-Zugangssteuerung zugelassen ist.
- Sie können die Kategorieberechtigung für einzelne Internetadressen außer Kraft setzen, indem Sie sie mit der gegenteiligen Berechtigungen im folgenden Bereich hinzufügen: **Internet-Zugangssteuerung > Einstellungen > Ausschlüsse**. Wenn eine Internetadresse durch die Internet-Kategorienfilter blockiert wird, können Sie für diese Adresse eine Web-Steuerung festlegen und die Berechtigung **Zulassen** erteilen.

Ausschlüsse

Sie können auch Internetregeln erstellen, um bestimmte Internet-Adressen konkret zu blockieren oder zuzulassen. Diese Regeln ignorieren die Einstellungen der Internet-Zugangssteuerung. Wenn also zum Beispiel der Internetzugang durch die Internet-Zugangssteuerung blockiert ist, können Benutzer trotzdem auf bestimmte Webseiten zugreifen.

So legen Sie eine Internetregel an:

1. Aktivieren Sie die Option **Ausschlüsse verwenden**.
2. Geben Sie die Adresse, die Sie zulassen oder blockieren möchten in das Feld **Internetadresse** ein.
3. Wählen Sie **Zulassen** oder **Blockieren** aus dem Menü **Berechtigung**.
4. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle, um die Adresse der Liste der Ausnahmen hinzuzufügen.
5. Klicken Sie auf **Speichern**.

So bearbeiten Sie eine Internet-Regel:

1. Klicken Sie auf die Internet-Adresse, die Sie bearbeiten wollen:
2. Die bestehende URL verändern.
3. Klicken Sie auf **Speichern**.

Um eine Internetregel zu entfernen, klicken Sie auf die entsprechende **×** **Löschen**-Schaltfläche.

Anwendungs-Blacklist

In diesem Bereich können Sie die Anwendungs-Blacklist konfigurieren, mit der Sie den Benutzerzugriff auf Anwendungen auf ihren jeweiligen Computern blockieren oder einschränken können. Sie können jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software.

So können Sie die Anwendungs-Blacklist konfigurieren:

1. Aktivieren Sie die Option **Anwendungs-Blacklist**.
2. Legen Sie die Anwendungen fest, auf die Sie den Zugriff beschränken möchten.
Um den Zugriff auf eine Anwendung einzuschränken:
 - a. Klicken Sie auf die Schaltfläche **+ Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.

- b. Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben. Dafür gibt es zwei Möglichkeiten:
- Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad im Bearbeitungsfeld nach Bedarf. So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%ProgramFiles` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
 - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein. Es empfiehlt sich, (nach Möglichkeit) **Systemvariablen** zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
- c. **Zugriffsplaner.** Legen Sie den Anwendungszugriff für bestimmte Tageszeiten während der Woche fest:
- Wählen Sie im Raster die Zeitintervalle, in denen der Zugriff auf die Anwendung blockiert werden soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.
 - Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.
 - Klicken Sie auf **Speichern**. Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle. Wenn Sie eine bestehende Regel bearbeiten möchten, klicken Sie auf die Regel, um das Konfigurationsfenster zu öffnen.

Datenschutz

Mit dem Identitätsschutz kann der Administrator Regeln definieren, die eine unautorisierte Weitergabe von sensiblen Daten verhindern.



Beachten Sie

Diese Funktion ist unter macOS nicht verfügbar.


Sie können Regeln erstellen, um personenbezogene oder vertrauliche Daten jeder Art zu schützen, so zum Beispiel:

- Persönliche Kundeninformationen
- Namen und Schlüsseldaten von Entwicklungsprodukten und -technologien
- Kontaktinformationen von Führungskräften im Unternehmen

Geschützte Informationen können Namen, Telefonnummern, Kreditkarten- und Bankdaten, E-Mail-Adressen usw. sein.

Basierend auf den von Ihnen erstellten Identitätsschutzregeln scannt Bitdefender Endpoint Security Tools den Web- und ausgehenden E-Mail-Verkehr nach bestimmten Zeichenfolgen (z. B. Kreditkartennummern). Wird eine Übereinstimmung gefunden, wird die entsprechende Webseite oder E-Mail-Nachricht blockiert, um zu verhindern, dass geschützte Daten versendet werden. Der Benutzer wird sofort über eine Benachrichtigungsseite im Browser oder eine E-Mail über die von Bitdefender Endpoint Security Tools durchgeführte Aktion informiert.

So konfigurieren Sie den Identitätsschutz:

1. Markieren Sie das Kästchen, um den Identitätsschutz einzuschalten.
2. Legen Sie Identitätsschutzregeln für alle sensiblen Daten an, die Sie schützen möchten. Um eine Regel anzulegen:
 - a. Klicken Sie auf die Schaltfläche  **Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
 - b. Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll. Wählen Sie einen eindeutigen Namen, damit Sie oder andere Administratoren die Regel entsprechend zuordnen können.
 - c. Bitte wählen Sie die zu sichernden Daten.
 - d. Geben Sie die Daten ein, die Sie schützen möchten (so zum Beispiel die Telefonnummer einer Führungskraft oder den internen Namen eines neuen Produkts in der Entwicklungsphase). Jede beliebige Kombination von Wörtern, Zahlen oder Zeichenfolgen aus alphanumerischen Zeichen und Sonderzeichen (z.B. @, # oder \$) ist möglich.

Geben Sie mindestens fünf Zeichen ein, um ein versehentliches Blockieren von E-Mail-Nachrichten oder Webseiten zu verhindern.



Wichtig

Eingegebene Daten werden verschlüsselt auf geschützten Endpunkten gespeichert, können aber über Ihr Control Center-Konto angezeigt werden. Für noch bessere Sicherheit sollten Sie die Daten, die Sie schützen möchten, nicht vollständig eingeben. In diesem Fall müssen Sie die Option **Ganze Wörter abgl.** deaktivieren.

- e. Konfigurieren Sie den Datenverkehrs-Scan nach Ihren Anforderungen.

- **Web-Datenverkehr (HTTP) scannen** - Scannt den HTTP- (Web-) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **E-Mail-Verkehr (SMTP) scannen** - Scannt den SMTP- (E-Mail-) Datenverkehr und blockiert alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.

Sie können wählen, ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

- f. Klicken Sie auf **Speichern**. Die neue Regel wird der Liste hinzugefügt.
3. Konfigurieren Sie Ausschlüsse für die Identitätsschutzregeln, damit Benutzer weiterhin geschützte Daten an autorisierte Webseiten und Empfänger versenden können. Ausschlüsse können global (auf alle Regeln) oder nur auf bestimmte Regeln angewendet werden. Um einen Ausschluss hinzuzufügen:
 - a. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
 - b. Geben Sie die Web- oder E-Mail-Adresse ein, an die Benutzer geschützte Daten weitergeben dürfen.
 - c. Wählen Sie die Art des Ausschlusses (Web- oder E-Mail-Adresse).
 - d. Wählen Sie aus der Tabelle **Regeln** die Identitätsschutzregel(n), auf die dieser Ausschluss angewendet werden soll.
 - e. Klicken Sie auf **Speichern**. Die neue Ausschlussregel wird der Liste hinzugefügt.



Beachten Sie

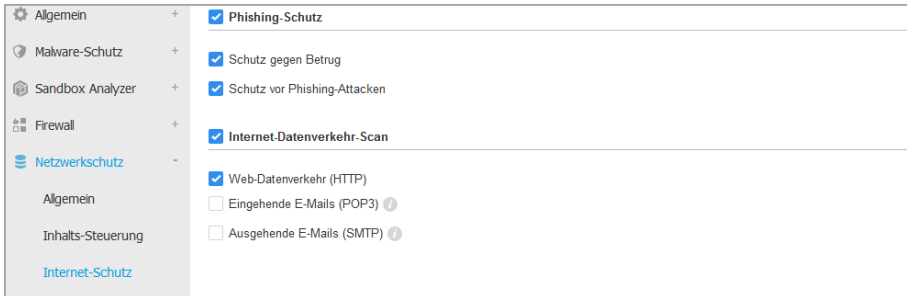
Wird eine E-Mail mit blockierten Inhalten an mehrere Empfänger adressiert, wird die Nachricht an die Empfänger verschickt, für die Ausschlüsse definiert wurden.

Um eine Regel oder einen Ausschluss aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche **⊗ Löschen** auf der rechten Seite der Tabelle.

Internet-Schutz

Auf dieser Seite sind die Einstellungen in die folgenden Bereiche eingeteilt:

- [Phishing-Schutz](#)
- [Internet-Datenverkehr-Scan](#)



Richtlinien für Computer und virtuelle Maschinen - Netzwerkschutz - Internet-Schutz

Phishing-Schutz

Der Phishing-Schutz blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben. Anstelle der Phishing-Seite wird eine spezielle Warnseite im Browser eingeblendet, die den Benutzer darüber informiert, dass die angeforderte Webseite gefährlich ist.


Wählen Sie **Phishing-Schutz**, um den Phishing-Schutz zu aktivieren. Sie können den Phishing-Schutz über die folgenden Einstellungen an Ihre Bedürfnisse anpassen:

- **Schutz vor Betrug.** Wählen Sie diese Option, wenn Sie den Schutz auf weitere Betrugsarten neben Phishing ausweiten möchten. So zum Beispiel Webseiten von Scheinfirmen, die zwar nicht direkt private Informationen anfordern, aber versuchen, sich als legitime Unternehmen auszugeben und Geld verdienen, indem Sie Menschen so manipulieren, dass Sie eine Geschäftsbeziehung mit ihnen aufnehmen.
- **Schutz vor Phishing-Attacken.** Lassen Sie diese Option aktiviert, um Benutzer vor Phishing-Versuchen zu schützen.

Wenn eine legitime Webseite fälschlicherweise als Phishing-Seite identifiziert und blockiert wird, können Sie diese zur Whitelist hinzufügen, damit Benutzer darauf zugreifen können. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

So verwalten Sie Phishing-Schutz-Ausnahmen:


1. Rufen Sie Einstellungen **Allgemein** auf und klicken Sie auf **Globale Ausschlüsse**.

2. Geben Sie die Internet-Adresse ein und klicken Sie auf die Schaltfläche  **Hinzufügen**.

Wenn Sie eine ganze Website ausschließen möchten, geben Sie den Domainnamen, z. B. `http://www.website.com`, ein; wenn Sie nur eine bestimmte Webseite ausschließen möchten, geben Sie die genaue Internetadresse dieser Seite ein.

**Beachten Sie**

Platzhalter in URLs sind nicht erlaubt.

3. Um eine Ausnahme aus der Liste zu löschen, klicken Sie auf die entsprechende  **Löschen**-Schaltfläche.
4. Klicken Sie auf **Speichern**.

Internet-Datenverkehr-Scan

Eingehende E-Mails (POP3) und der Internet-Datenverkehr werden in Echtzeit gescannt, um zu verhindern, dass Malware auf den Endpunkt heruntergeladen wird. Ausgehende E-Mails (SMTP) werden gescannt, um zu verhindern, dass Malware andere Endpunkte infiziert. Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

Wenn eine infizierte E-Mail erkannt wird, wird diese automatisch mit einer Standard-E-Mail ersetzt, die den Empfänger über die ursprüngliche infizierte E-Mail informiert. Wenn eine Webseite Malware enthält oder verbreitet, wird diese automatisch blockiert. Anstelle der Webseite wird eine Warnung angezeigt, die den Anwender darüber informiert, dass die aufgerufene Seite gefährlich ist.

Sie können zur Steigerung der Systemleistung das Scannen des E-Mail- und Internet-Datenverkehrs deaktivieren, dies wird aber nicht empfohlen. Dabei handelt es sich nicht um eine ernstzunehmende Bedrohung, solange die Zugriff-Scans für lokale Dateien aktiviert bleiben.

**Beachten Sie**

Die Optionen **Eingehende E-Mails** und **Ausgehende E-Mails** sind unter macOS nicht verfügbar.

Netzwerkangriffe

Das Network Attack Defense-Modul fügt eine weitere Sicherheitsebene hinzu. Diese basiert auf einer Bitdefender-Technologie zur Erkennung von Angriffen auf das Netzwerk, mit denen versucht wird, über Verfahren wie Brute-Force-Angriffe, Netzwerk-Exploits und Passwortdiebstahl Zugriff auf Endpunkte zu erlangen.

The screenshot shows the configuration page for Network Attack Defense. On the left is a navigation menu with categories like 'Allgemein', 'Malware-Schutz', 'Sandbox Analyzer', 'Firewall', 'Netzwerkschutz', and 'Patch-Verwaltung'. The 'Netzwerkschutz' section is expanded to show 'Allgemein', 'Inhalts-Steuerung', 'Internet-Schutz', and 'Netzwerkangriffe'. The 'Netzwerkangriffe' section is active, showing a checkbox for 'Network Attack Defense' which is checked. Below this is a description: 'Bei dieser Funktion handelt es sich um eine Sicherheitsschicht zur Erkennung von Netzwerkangriffsverfahren, die versuchen, sich über Anforderungen Ihres Unternehmens anzupassen.' Underneath is a table of attack techniques with checkboxes and dropdown menus for each.

Angriffstechniken	
<input checked="" type="checkbox"/>	Erstzugriff Blockieren
<input checked="" type="checkbox"/>	Zugangsdatenklau Blockieren
<input checked="" type="checkbox"/>	Ausspähen Blockieren
<input checked="" type="checkbox"/>	Laterale Bewegung Blockieren
<input checked="" type="checkbox"/>	Crimeware Blockieren

[Auf Standard zurücksetzen](#)

Richtlinien für Computer und virtuelle Maschinen - Netzwerkschutz - Netzwerkangriffe

So konfigurieren Sie Network Attack Defense:

1. Markieren Sie das Kontrollkästchen **Network Attack Defense**, um das Modul zu aktivieren.
2. Markieren Sie die entsprechenden Kontrollkästchen, um den Schutz vor der jeweiligen Netzwerkangriffskategorie zu aktivieren. In der ATT&CK-Datenbank von MITRE sind die Netzwerkangriffstechniken wie folgt aufgeteilt:
 - **Erster Zugriff** - Der Angreifer verschafft sich auf verschiedene Weisen Zugang zu einem Netzwerk, so zum Beispiel über Sicherheitslücken in öffentlich zugänglichen Webservern. Beispiele: Information Disclosure Exploits, SQL Injection Exploits, Drive-by Download Injection-Vektoren.
 - **Zugriff auf Anmeldedaten** - Der Angreifer erbeutet Zugangsdaten wie Benutzernamen und Passwörter, um Zugang zu den Systemen zu erhalten. Beispiele: Brute-Force-Angriffe, unbefugte Authentifizierungsangriffe, Passwortdiebstahl.
 - **Erkennung** - Der Angreifer versucht nach dem Eindringen Informationen über die Systeme und das interne Netzwerk zu ermitteln, bevor er über seine

weiteren Schritte entscheidet. Beispiele: Directory Traversal Exploits, HTTP Directory Traversal Exploits.

- **Laterale Bewegungen** - Der Angreifer erkundet das Netzwerk, meist indem er sich von System zu System bewegt, um sein Hauptziel zu finden. Zur Erreichung seiner Ziele kann der Angreifer dabei spezifische Tools einsetzen. Beispiele: Command Injection Exploits, Shellshock Exploits, Double Extension Exploits.
 - **Crimeware** - Diese Kategorie umfasst Verfahren, mit denen Cyberkriminelle ihr Vorgehen automatisieren. Crimeware-Verfahren umfassen zum Beispiel Nuclear Exploits und verschiedene Malware-Varianten wie Trojaner und Bots.
3. Wählen Sie aus den folgenden Optionen die Aktionen aus, die Sie für jede Kategorie von Netzwerkangriffstechniken durchführen möchten:
- a. **Blockieren** - Die Network Attack Defense stoppt den Angriffsversuch, sobald er erkannt wurde.
 - b. **Nur Bericht** - Die Network Attack Defense informiert Sie über den erkannten Angriffsversuch, versucht aber nicht, ihn zu stoppen.

Mit einem Klick auf die Schaltfläche **Standard wiederherstellen** unten auf der Seite können Sie jederzeit die Standardeinstellungen wiederherstellen.

Sie finden Details zu Netzwerkangriffsversuchen im Bericht Netzwerkvorfälle und in der Ereignisbenachrichtigung Netzwerkvorfälle.

7.2.7. Patch-Verwaltung



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

Mit dem Modul Patch-Verwaltung müssen Sie sich nicht mehr selbst darum kümmern, dass die Endpunkte stets mit den aktuellsten Software-Patches auf dem neuesten Stand gehalten werden. Es sorgt für die automatische Verteilung und Installation von Patches für eine Vielzahl an Produkten.



Beachten Sie

In diesem Artikel in der Wissensdatenbank finden Sie eine Liste mit allen unterstützten Anbietern und Produkten.

In diesem Richtlinienbereich finden Sie die Einstellungen für die automatische Bereitstellung von Patches. Zunächst legen Sie fest, wie die Patches auf die Endpunkte heruntergeladen werden. Im Anschluss konfigurieren Sie die Art und den Zeitpunkt der zu installierenden Patches.

Konfigurieren der Patch-Download-Einstellungen

Bei der Patch-Verteilung kommen zur Optimierung des Netzwerkdatenverkehrs die Patch-Cache-Server zum Einsatz. Die Endpunkte verbinden sich mit diesen Servern und laden die Patches über das lokale Netzwerk herunter. Um die Hochverfügbarkeit der Patches sicherzustellen, wird die Nutzung von mehreren Servern empfohlen.

Gehen Sie folgendermaßen vor, um den Zielendpunkten Patch-Cache-Server zuzuweisen:

1. Klicken Sie im Bereich **Patch-Download-Einstellungen** auf das Feld am oberen Rand der Tabelle. Die Liste der gefundenen Patch-Cache-Server wird angezeigt. Ist die Liste der leer, müssen Sie zunächst die Patch-Cache-Server-Rolle auf Relais in Ihrem Netzwerk installieren. Weitere Informationen hierzu finden Sie in der Installationsanleitung.
2. Wählen Sie den gewünschten Server aus der Liste aus.
3. Klicken Sie auf den Button **+**Hinzufügen.
4. Wiederholen Sie die vorausgegangenen Schritte, um bei Bedarf weitere Server hinzuzufügen.
5. Verwenden Sie die Pfeile rechts neben der Tabelle, um die Priorität der Server festzulegen. Dabei nimmt die Priorität von oben nach unten ab.

Die Endpunkte fordern die Patches von den zugewiesenen Servern nach Reihenfolge der festgelegten Priorität ab. Die Endpunkte laden ein Patch von dem Server herunter, auf dem der Patch zuerst gefunden wird. Ein Server, auf dem ein angefordertes Patch nicht vorliegt, wird dieses Patch automatisch vom Anbieter heruntergeladen, um es für zukünftige Anfragen verfügbar zu machen.

Um nicht mehr benötigte Server zu löschen, klicken Sie auf die entsprechende **-** Löschen-Schaltfläche auf der rechten Seite der Tabelle.

Markieren Sie die Option **Anbieter-Websites als Ausweichadresse für den Patch-Download verwenden**, um sicherzustellen, dass Ihre Endpunkte auch dann mit Software-Patches versorgt werden, wenn die Patch-Cache-Server nicht verfügbar sind.

Konfigurieren von Patch-Scan und -Installationen

GravityZone führt jede Installation in zwei eigenständigen Phasen durch:

1. Bewertung. Nach Anforderung durch die Managementkonsole suchen die Endpunkte nach fehlenden Patches und melden diese zurück.
2. Installation. Die Konsole übermittelt an die Agenten eine Liste mit den Patches, die Sie installieren möchten. Der Endpunkt lädt daraufhin die Patches vom Patch-Cache-Server herunter und installiert sie.

Über die Richtlinie werden die Einstellungen zur vollständigen oder teilweisen Automatisierung dieser Prozesse festgelegt, damit diese regelmäßig nach dem vorgegebenen Zeitplan durchgeführt werden können.

Gehen Sie folgendermaßen vor, um automatische Patch-Scans einzurichten:

1. Markieren Sie das Kästchen **Automatischer Patch-Scan**.
2. Verwenden Sie die Planungsoptionen, um die Scan-Wiederholung zu konfigurieren. Scans können täglich oder an bestimmten Wochentagen jeweils zu einer bestimmten Zeit durchgeführt werden.
3. Wählen Sie **Intelligenter Scan bei Installation einer neuen App/eines neuen Programms**, um die Installation neuer Anwendung auf einem Endpunkt zu erkennen und die dafür verfügbaren Patches zu suchen.

Gehen Sie folgendermaßen vor, um die automatische Patch-Installation zu konfigurieren:

1. Markieren Sie das Kästchen **Patches nach dem Scan automatisch installieren**.
2. Legen Sie fest, welche Patch-Typen installiert werden sollen: sicherheitsrelevante, nicht sicherheitsrelevante oder beides.
3. Verwenden Sie die Planungsoptionen, um festzulegen, wann die Installationsaufgaben durchgeführt werden sollen. Sie können festlegen, dass die Installation sofort nach Abschluss des Patch-Scans durchgeführt wird. Die Installation kann aber auch täglich oder an bestimmten Wochentagen jeweils zu einer bestimmten Zeit erfolgen. Wir empfehlen, sicherheitsrelevante Patches sofort nach deren Ermittlung zu installieren.

4. Standardmäßig kommen alle Produkte für die Installation von Patches infrage. Wenn Sie aber nur bestimmte, von Ihnen als geschäftskritisch eingestufte Produkte automatisch aktualisieren möchten, gehen Sie bitte folgendermaßen vor:
 - a. Markieren Sie das Kästchen **Bestimmter Anbieter und Produkt**.
 - b. Klicken Sie am oberen Rand der Tabelle auf das Feld **Anbieter**. Eine Liste mit allen unterstützten Anbietern wird angezeigt.
 - c. Scrollen Sie durch die Liste und wählen Sie den Anbieter der Produkte aus, die Sie patchen möchten.
 - d. Klicken Sie am oberen Rand der Tabelle auf das Feld **Produkte**. Eine Liste mit allen Produkten des ausgewählten Anbieters wird angezeigt.
 - e. Wählen Sie alle Produkte aus, die Sie patchen möchten.
 - f. Klicken Sie auf den Button **+Hinzufügen**.
 - g. Wiederholen Sie die vorausgegangenen Schritte für alle weiteren Anbieter und Produkte.

Falls Sie vergessen haben, ein Produkt hinzuzufügen oder ein Produkt entfernen möchten, suchen Sie den Anbieter in der Tabelle, doppelklicken Sie auf **Produkte** und markieren Sie das Produkt in der Liste bzw. heben Sie die Markierung auf.

Um einen Anbieter und alle dazugehörigen Produkte zu entfernen, suchen Sie diesen Anbieter in der Liste und klicken Sie auf die entsprechende **- Löschen**-Schaltfläche auf der rechten Seite der Tabelle.

5. Ein Endpunkt kann aus verschiedenen Gründen zum geplanten Zeitpunkt der Patch-Installation offline sein. Markieren Sie die Option **Falls verpasst, so schnell wie möglich nachholen**, um die Patches zu installieren, sobald der Endpunkt wieder online ist.
6. Manche Patches machen einen Neustart des Systems zum Abschluss der Installation erforderlich. Falls Sie dies lieber manuell durchführen möchten, markieren Sie die Option **Neustart aufschieben**.



Wichtig

Für eine erfolgreiche Bewertung und Installation auf Windows-Endpunkten, müssen die folgenden Anforderungen erfüllt sein:

- Das **DigiCert Assured ID Root CA-Zertifikat** ist unter **Vertrauenswürdige Stammzertifizierungsstellen** gespeichert.
- **Vorübergehende Zertifizierungsstellen** umfasst das **DigiCert SHA2 Assured ID Code Signing CA-Zertifikat**.
- Auf den Endpunkten sind die Patches für Windows 7 und Windows Server 2008 R2 installiert, die in diesem Microsoft-Artikel erwähnt sind: [Microsoft Security Advisory 3033929](#)

7.2.8. Anwendungssteuerung



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

Das Anwendungssteuerungsmodul sorgt für noch besseren Schutz vor verschiedensten Malware-Bedrohungen (Ransomware, Zero-Day-Angriffe, Exploits in Drittanwendungen, Trojaner, Spyware, Rootkits, Adware usw.), indem es die Ausführung von nicht autorisierten Anwendungen und Prozessen verhindert. Die Anwendungssteuerung verkleinert die Angriffsfläche für Malware-Bedrohungen auf dem Endpunkt und verhindert die Installation und Ausführung von nicht erwünschten, nicht vertrauenswürdigen oder schädlichen Anwendungen.

Mit der Anwendungssteuerung können flexible Richtlinien für das Whitelisting von Anwendungen und die Verwaltung von Update-Berechtigungen angewandt werden.



Anwendungssteuerung



Wichtig

- Führen Sie zur Aktivierung der **Anwendungssteuerung** für ihre aktuell installieren Clients die Aufgabe **Client neu konfigurieren** aus. Nach der Installation des Moduls können Sie seinen Status in Fenster **Informationen** einsehen.

- Die Anwendungssteuerung hat nach Anwendungs-Updates erhebliche Auswirkungen auf den Power-User-Modus. Wird zum Beispiel eine Anwendung auf der Whitelist aktualisiert, übermittelt der Endpunkt die neuen Informationen. GravityZone aktualisiert die Regel mit den neuen Werten und übermittelt die Richtlinie erneut.

Führen Sie die Aufgabe **Anwendungserkennung** aus, um die in Ihrem Netzwerk ausgeführten Anwendungen und Prozesse anzuzeigen. Weitere Informationen finden Sie unter „**Anwendungserkennung**“ (S. 103). Im Anschluss können Sie die Regeln für die Anwendungssteuerung festlegen.

Für die Anwendungssteuerung gibt es zwei Modi:

- **Testmodus.** Die Anwendungssteuerung erkennt und informiert nur über die Anwendungen in der Control Center und lässt sie weiterhin laufen. Sie können Ihre Whitelist-Regeln und Richtlinien konfigurieren und testen, es werden jedoch keine Anwendungen blockiert.
- **Produktivmodus.** Die Anwendungssteuerung blockiert alle unbekanntes Anwendungen. Prozesse des Microsoft-Betriebssystems sowie Bitdefender-Prozesse werden standardmäßig in die Whitelist aufgenommen. Anwendungen, die in die Whitelist aufgenommen wurden, dürfen ausgeführt werden. Um Anwendungen auf der Whitelist aktualisieren zu können, müssen Sie zunächst Updater festlegen. Dabei handelt es sich um festgelegte Prozesse, denen es erlaubt wird, Veränderungen an bestehenden Anwendungen vorzunehmen. Weitere Informationen finden Sie unter „**Anwendungsbestand**“ (S. 199).

Warnung

- Um sicherzustellen, dass unbedenkliche Anwendungen nicht durch die Anwendungssteuerung beeinträchtigt werden, müssen Sie die Anwendungssteuerung zunächst im Testmodus laufen lassen. So können Sie sicherstellen, dass die Whitelist-Regeln und Richtlinien in Ihrem Sinne festgelegt wurden.
- Prozesse, die bereits ausgeführt werden, wenn die Anwendungssteuerung in den **Produktivmodus** versetzt wird, werden nach dem nächsten Neustart des Prozesses blockiert.

So können Sie die Berechtigungen zum Ausführen von Anwendungen verwalten:

1. Markieren Sie das Kästchen **Anwendungssteuerung**, um dieses Modul zu aktivieren.
2. Über das Kästchen **Im Testmodus ausführen** können Sie den Testmodus aktivieren oder deaktivieren.



Beachten Sie

- Im Testmodus werden Sie informiert, wenn die Anwendungssteuerung eine bestimmte Anwendung blockiert hätte. Weitere Informationen finden Sie unter „[Benachrichtigungsarten](#)“ (S. 513).
- Die Benachrichtigung **Blockierte Anwendung** wird im Benachrichtigungsbereich angezeigt, wenn neue Anwendungen erkannt oder Anwendungen auf der Blacklist blockiert werden.

3. Legen Sie Prozessstartregeln fest.

Prozessstartregeln

Über die Anwendungssteuerung können Sie bestimmte Anwendungen und Prozesse manuell autorisieren. Dies kann anhand des Hash-Werts der ausführbaren Datei, des Fingerabdrucks unterzeichnenden Zertifikats oder des Pfads der Anwendung erfolgen. Sie können darüber hinaus Ausnahmen von den Regeln festlegen.





Beachten Sie

Um die individuellen Werte für den Hash der ausführbaren Datei und den Fingerabdruck der Zertifikatsnutzung zu ermitteln, verwenden Sie die „[Tools der Anwendungssteuerung](#)“ (S. 548)

In der Tabelle **Prozessstartregeln** finden Sie wichtige Informationen über bestehende Regeln:

- Regelpriorität. Je weiter oben eine Regel in der Liste steht, desto höher ist ihre Priorität.
- Regelname und Status.
- Zielanwendungen und ihre Ausführungsberechtigungen. Das Ziel beschreibt die Anzahl der Bedingungen, die erfüllt werden müssen, damit die Regel zur Anwendung kommt bzw. die Anzahl der Anwendungen oder Gruppen, auf die die Regel angewandt wird.

So können Sie eine Prozessstartregel anlegen:

1. Klicken Sie auf die Schaltfläche  **Hinzufügen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
2. Geben Sie im Bereich **Allgemein** einen **Regelnamen** ein.
3. Markieren Sie das Kästchen **Aktiviert**, um die Regel zu aktivieren.
4. Legen Sie im Bereich **Ziele** das Regelziel fest:
 - **Bestimmter Prozess oder Prozesse** zur Definition eines Prozesses, dessen Ausführung zugelassen oder verweigert werden soll. Die Autorisierung kann nach Pfad, Hash oder Zertifikat erfolgen. Die Regelbedingungen können über ein logisches UND verknüpft werden.
 - So können Sie eine Anwendung über einen bestimmten Pfad autorisieren:
 - a. Wählen Sie in der Spalte **Typ** den Eintrag **Pfad** aus. Geben Sie den Pfad zum Objekt an. Sie können einen absoluten oder relativen Pfadnamen eingeben oder Platzhalter verwenden. Das Sternchen (*) steht für jede Datei innerhalb eines Verzeichnisses. Zwei Sternchen (**) stehen für alle Dateien und Verzeichnisse im definierten Verzeichnis. Ein Fragezeichen (?) steht für genau ein beliebiges Zeichen. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.
 - b. Wählen Sie aus dem Klappmenü **Wählen Sie einen oder mehrere Kontexte aus**. lokal, CR-ROM, Wechselmedium oder Netzwerk aus. Sie können Anwendungen, die über Wechselmedien ausgeführt werden, blockieren oder ihre Ausführung nur lokal erlauben.
 - Um Anwendungen anhand ihres Hashs zu autorisieren, wählen Sie in der Spalte **Typ** den Eintrag **Hash** aus und geben Sie einen Hash-Wert ein. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.
 - **Wichtig**
 Zu Erzeugung des Hash-Werts können Sie das [Fingerprint-Tool](#) herunterladen. Weitere Informationen finden Sie unter „[Tools der Anwendungssteuerung](#)“ (S. 548)
 - Zur Autorisierung anhand eines Zertifikats wählen Sie in der Spalte **Typ** den Eintrag **Zertifikat** aus und geben Sie einen Zertifikatfingerabdruck

ein. Sie können zudem eine Beschreibung hinzufügen, um den Prozess besser zuordnen zu können.



Wichtig

Zum Erhalt des Zertifikatfingerabdrucks können Sie das [Thumbprint-Tool](#) herunterladen. Weitere Informationen finden Sie unter „[Tools der Anwendungssteuerung](#)“ (S. 548)

Allgemein

Name der Regel:

Aktiviert

Ziele

Ziel:

Zertifikat	Geben Sie einen Zertifikatfingerabdruck ein.	Geben Sie einen Wert ein.	Wählen Sie einen oder mehrere Kontexte.	
Typ	Übereinstimmung	Beschreibung	Kontext	Aktion
Pfad	C:\test**.exe	**wildcard	Lokal	⊗
Pfad	C:\test\test1*.exe	*wildcard	Lokal	⊗
Pfad	C:\test\test1\exemp?e.exe	? wildcard	Lokal	⊗
Hash	aabbccddeeffghh6789	hash beschreibung	N/A	⊗
Zertifikat	aaddggyy1234567890	zertifikat beschreibung	N/A	⊗

Anwendungsregeln

Klicken Sie auf **+** **Hinzufügen** die Regel hinzuzufügen.

- **Bestandsanwendungen oder -gruppen** zum Hinzufügen von im Ihrem Netzwerk ermittelten Gruppen oder Anwendungen. Sie können die in Ihrem Netzwerk ausgeführten Anwendungen auf der Seite **Netzwerk- > Anwendungsbestand** einsehen. Weitere Informationen finden Sie unter „[Anwendungsbestand](#)“ (S. 199).

Geben Sie die Namen der Anwendungen oder Gruppen durch Komma getrennt in das Feld ein. Die Funktion zum automatischen Einfügen zeigt schon während der Eingabe Vorschläge an.

5. Markieren Sie das Kästchen **Auch untergeordnete Prozesse**, um die Regel auch auf Kindprozesse anzuwenden.



Warnung



Wir empfehlen, diese Option bei der Festlegung von Regeln für Browser-Anwendungen zu deaktivieren, um Sicherheitsrisiken zu vermeiden.

6. Sie können optional auch Ausschlüsse von der Prozessstartregel festlegen. Das Hinzufügen ähnelt der bereits im beschriebenen Vorgehensweise.
7. Im Bereich **Berechtigungen** legen Sie fest, ob die Regelausführung zugelassen oder verweigert werden soll.
8. Klicken Sie **Speichern**, um die Änderungen zu speichern.


So bearbeiten Sie eine bestehende Regel:

1. Klicken Sie auf den Namen der Regel, um das Konfigurationsfenster zu öffnen.
2. Geben Sie neue Werte für die Optionen ein, die Sie ändern möchten.
3. Klicken Sie **Speichern**, um die Änderungen zu speichern.

So können Sie die Regelpriorität festlegen:

1. Markieren Sie das Kästchen der gewünschten Regel.
2. Klicken Sie auf die Prioritätsschaltflächen auf der rechten Seite der Tabelle:
 - Über die Schaltfläche  **Hoch** erhöhen Sie die Priorität der ausgewählten Regel.
 - Mit der Schaltfläche  **Runter** verringern Sie die Priorität.

Sie können Regeln einzeln oder als Gruppe löschen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie die Regeln aus, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle. Eine gelöschte Regel kann nicht wiederhergestellt werden.

7.2.9. Gerätesteuerung



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations

- Windows für Server
- macOS

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausschlüssen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich.

! Wichtig

Unter macOS ist für die Gerätesteuerung eine Kernel-Erweiterung erforderlich. Die Installation einer Kernel-Erweiterung erfordert unter macOS High Sierra (10.13) und höher die Zustimmung des Benutzers. Das System benachrichtigt den Benutzer, dass eine Bitdefender-Systemerweiterung blockiert wurde. Der Benutzer kann die Zustimmung dazu in den Einstellungen unter **Sicherheit & Datenschutz** erteilen. Dieses Modul funktioniert erst, wenn der Benutzer der Bitdefender-Systemerweiterung zugestimmt hat. Bis dahin wird in der Endpoint Security for Mac-Benutzeroberfläche ein kritisches Problem angezeigt und die Zustimmung angefordert.

Um den Benutzern Aufwand zu ersparen, kann die Bitdefender-Kernelerweiterung auch im Voraus genehmigt werden, indem sie mithilfe eines Mobilgerät-Verwaltungstools auf die Whitelist gesetzt wird. Weitere Details zu Bitdefender-Kernelerweiterungen finden Sie in [diesem Artikel](#).

Um das Modul Gerätesteuerung nutzen zu können, müssen Sie es zunächst im auf den gewünschten Endpunkten installierten Sicherheitsagenten integrieren und anschließend die Option **Gerätesteuerung** in der Richtlinie, die diesen Endpunkten zugewiesen ist, aktivieren. Ab dann wird der Sicherheitsagent jedes Mal, wenn ein Gerät an einen verwalteten Endpunkt angeschlossen wird, Informationen über dieses Ereignis an das Control Center senden. Die gesendeten Informationen enthalten den Namen des Geräts, die Klasse, die ID und den Zeitpunkt, zu dem das Gerät angeschlossen wurde.

In der nachfolgenden Tabelle finden Sie die von der Gerätesteuerung auf Windows- und macOS-Systemen unterstützten Gerätetypen:

Gerätetyp	Windows	macOS
Bluetooth-Adapter	x	x
CR-ROM-Geräte	x	x
Diskettenlaufwerke	x	N/A
IEEE 1284.4	x	

Gerätetyp	Windows	macOS
IEEE 1394	x	
Bildgebende Geräte	x	x
Modems	x	Verwaltet unter Netzwerkadapter
Bandlaufwerke	x	N/A
Windows Mobile	x	x
COM/LPT-Ports	x	LPT auf serielle Anschlüsse wird unterstützt
SCSI Raid	x	
Drucker	x	Unterstützt nur lokal verbundene Drucker
Netzwerkkarte	x	X (einschl. WLAN-Dongles)
WLAN-Netzwerkkarten	x	x
Interner Speicher	x	
Externer Speicher	x	x



Beachten Sie

- Wenn unter macOS die Berechtigung **Benutzerdef.** für eine bestimmte Geräteklasse ausgewählt ist, gilt nur die für die Unterkategorie **Sonstige** konfigurierte Berechtigung.
- Unter Windows und macOS erlaubt oder verweigert die Gerätesteuerung je nach Richtlinie den Zugriff auf den gesamten Bluetooth-Adapter auf Systemebene. Es besteht keine Möglichkeit, detaillierte Ausschlüsse für ein gekoppeltes Gerät festzulegen.

Mit der Gerätesteuerung können Sie Berechtigungen von Geräten auf zwei Arten verwalten:

- [Berechtigungsregeln definieren](#)
- [Berechtigungsausschlüsse definieren](#)

Regeln

Im Bereich **Regeln** können die Berechtigungen für die mit den Zielendpunkten verbundenen Geräte definiert werden.

So legen Sie die Berechtigungen für einen bestimmten Gerätetyp fest:

1. Gehen Sie zu **Gerätesteuerung > Regeln**.
2. Klicken Sie in der Tabelle auf den Gerätenamen.
3. Wählen Sie einen Berechtigungstyp aus den verfügbaren Optionen. Die verfügbaren Berechtigungen hängen dabei vom Gerätetyp ab:
 - **Zugelassen:** Das Gerät kann auf dem Endpunkt verwendet werden.
 - **Blockiert:** Das Gerät kann nicht auf dem Endpunkt verwendet werden. In diesem Fall gibt der Sicherheitsagent jedes Mal, wenn das Gerät mit dem Endpunkt verbunden wird, eine Meldung aus, die besagt, dass das Gerät blockiert wurde.



Wichtig

Verbundene Geräte, die zuvor blockiert wurden, werden nicht automatisch entblockiert, wenn die Berechtigung auf **Zugelassen** gesetzt wird. Der Benutzer muss das System neu starten oder das Gerät erneut verbinden, um es verwenden zu können.

- **Schreibgeschützt:** Von dem Gerät kann nur gelesen werden.
- **Benutzerdefiniert:** Für jede Art von Anschluss desselben Gerätes, wie Firewire, ISA Plug & Play, PCI, PCMCIA, USB usw., können unterschiedliche Berechtigungen definiert werden. In diesem Fall wird die Liste der für das ausgewählte Gerät verfügbaren Komponenten angezeigt, und Sie können für jede Komponente eine eigene Berechtigung festlegen.

Für externe Speichermedien können Sie zum Beispiel nur USB blockieren und alle anderen Anschlussarten zulassen.

Externer Speicher Regel ✕

Berechtigung: * ▼

Beschreibung: *

Benutzerdefinierte Berechtigungen

Firewire: ▼

ISA Plug & Play: ▼

PCI: ▼

PCMCIA: ▼

SCSI: ▼

SD-Karte: ▼

USB: ▼

Other: ▼

Richtlinien für Computer und virtuelle Maschinen – Gerätesteuerung – Regeln


Ausschlüsse

Nachdem Sie die Berechtigungsregeln für verschiedene Gerätetypen festgelegt haben, möchten Sie eventuell bestimmte Geräte oder Produktarten von diesen Regeln ausschließen.

Geräteausschlüsse können Sie auf eine von zwei Arten definieren:

- Nach Geräte-ID (oder Hardware-ID); so können konkrete Einzelgeräte ausgeschlossen werden.
- Nach Produkt-ID (oder PID); so können Geräteserien desselben Herstellers ausgeschlossen werden.

So definieren Sie Geräteregelausschlüsse:

1. Gehen Sie zu **Gerätesteuerung > Ausschlüsse**.
2. Aktivieren Sie die Option **Ausschlüsse**.
3. Klicken Sie auf die Schaltfläche  **Hinzufügen** am oberen Ende der Tabelle.

4. Wählen Sie, auf welche Art Sie Ausschlüsse hinzufügen möchten:

- **Manuell.** Mit dieser Methode müssen Sie jede einzelne Geräte-ID oder Produkt-ID, die Sie ausschließen möchten, zur Hand haben und einzeln eingeben:
 - a. Wählen Sie den Ausschlusstyp (nach Produkt-ID oder nach Geräte-ID).
 - b. Geben Sie im Feld **Ausnahmen** die IDs ein, die Sie ausschließen möchten:
 - c. Geben Sie im Feld **Beschreibung** einen aussagekräftigen Namen ein, anhand dessen Sie das Gerät oder die Geräteserie wiedererkennen können.
 - d. Wählen Sie den Berechtigungstyp für die entsprechenden Geräte (**Zugelassen** oder **Blockiert**).
 - e. Klicken Sie auf **Speichern**.



Beachten Sie

Sie können Ausschlüsse auch manuell über die Geräte-ID konfigurieren. Verwenden Sie dazu die Syntax `wildcards:Geräte-ID`. In der Geräte-ID kann mit einem Fragezeichen (?) ein Zeichen ersetzt werden und mit einem Sternchen (*) beliebig viele Zeichen. Mit `wildcards:PCI\VEN_8086*` werden z. B. alle Geräte von der Richtlinienregel ausgeschlossen, die in ihrer ID die Zeichenfolge `PCI\VEN_8086` haben.

- **Von gefundenen Geräten.** Mit dieser Methode können Sie die Geräte-IDs oder Produkt-IDs, die Sie ausschließen möchten, aus einer Liste aller in Ihrem Netzwerk gefundenen Geräte auswählen (nur verwaltete Endpunkte):
 - a. Wählen Sie den Ausschlusstyp (nach Produkt-ID oder nach Geräte-ID).
 - b. Wählen Sie aus der Tabelle **Ausschlüsse** die IDs, die Sie ausschließen möchten:
 - Bei Ausschluss nach Geräte-ID müssen Sie jedes einzelne Gerät in der Liste auswählen, das Sie ausschließen möchten.
 - Bei Ausschluss nach Produkt-ID können Sie ein Gerät auswählen und damit alle Geräte mit dieser Produkt-ID ausschließen.
 - c. Geben Sie im Feld **Beschreibung** einen aussagekräftigen Namen ein, anhand dessen Sie das Gerät oder die Geräteserie wiedererkennen können.
 - d. Wählen Sie den Berechtigungstyp für die entsprechenden Geräte (**Zugelassen** oder **Blockiert**).
 - e. Klicken Sie auf **Speichern**.



Wichtig

- Geräte, die bei der Installation von Bitdefender Endpoint Security Tools bereits mit den Endpunkten verbunden waren, werden erst nach einem Neustart der entsprechenden Endpunkte gefunden.
- Verbundene Geräte, die zuvor blockiert wurden, werden nicht automatisch entblockiert, wenn eine Ausnahme mit der Berechtigung **Zugelassen** gesetzt wird. Der Benutzer muss das System neu starten oder das Gerät erneut verbinden, um es verwenden zu können.

Alle Geräteausschlüsse werden in der Tabelle **Ausschlüsse** aufgeführt.

So entfernen Sie einen Ausschluss:

1. Markieren Sie den Ausschluss in der Tabelle.
2. Klicken Sie auf die Schaltfläche **+ Löschen** am oberen Rand der Tabelle.

Regeltyp	Ausnahme	Beschreibung	Berechtigung	
<input type="checkbox"/>	Geräte-ID	USB\VID_0C45&PID_641&REV	Web Cam	Zugelassen
<input type="checkbox"/>	Produkt ID	8192	AMD Ethernet Adapters	Zugelassen

Richtlinien für Computer und virtuelle Maschinen – Gerätesteuerung – Ausschlüsse

7.2.10. Relais



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server
- Linux

In diesem Bereich können Sie Kommunikations- und Update-Einstellungen für Endpunkte mit Relais-Rolle definieren.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [Kommunikationsserver](#)
- [Update \(Aktualisierung\)](#)

Kommunikationsserver

Im Reiter **Kommunikation** finden Sie Proxy-Einstellungen für die Kommunikation zwischen Relais-Endpunkten und den GravityZone-Komponenten.

Bei Bedarf können Sie die Kommunikation zwischen einzelnen Relais-Endpunkten und Bitdefender Cloud Services/GravityZone mit den folgenden Einstellungen einzeln konfigurieren:

- **Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.
- **Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich [Allgemein > Einstellungen](#) definiert sind.
- **Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den Bitdefender-Komponenten kommunizieren.

Update (Aktualisierung)

In diesem Bereich können Sie die Update-Einstellungen für Endpunkte mit Relais-Rolle definieren:

- Im Bereich **Update** können Sie die folgenden Einstellungen konfigurieren:
 - Der zeitliche Abstand, in dem die Relais-Endpunkte nach Updates suchen.
 - Der Ordner auf dem Relais-Endpunkt, in dem die Produkt- und Signatur-Updates gespeichert und gespiegelt werden. Wenn Sie einen bestimmten Download-Ordner festlegen möchten, geben Sie einfach den vollständigen Pfad in das entsprechende Feld ein.



Wichtig

Es empfiehlt sich, einen Ordner festzulegen, der nur für Produkt- und Signatur-Updates da ist. Ein Ordner, in dem auch Systemdateien oder private Dateien liegen, sollte nicht gewählt werden.

- **Benutzerdefinierte Update-Server festlegen.** Der Standard-Update-Server für Relais-Agenten ist der lokale GravityZone-Update-Server. Sie können einen anderen Update-Server festlegen, indem Sie die IP-Adresse oder den lokalen

Hostnamen einer oder mehrerer Update-Server in Ihrem Netzwerk eingeben und dann deren Priorität mithilfe der Pfeile festlegen, die angezeigt werden, wenn Sie mit dem Mauszeiger auf den jeweiligen Server gehen. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

So definieren Sie einen benutzerdefinierten Update-Server:

1. Aktivieren Sie die Option **Benutzerdefinierte Update-Server festlegen**.
2. Geben Sie die Adresse des neuen Update-Servers in das Feld **Ziel hinzufügen** ein. Verwenden Sie dazu eine der folgenden Syntaxoptionen:
 - update_server_ip:port
 - update_server_name:port

Der Standard-Port ist 7074.

3. Falls der Relais-Endpoint über einen Proxy-Server mit dem lokalen Update-Server kommuniziert, aktivieren Sie **Proxy benutzen**. Die Proxy-Einstellungen, die im Bereich **Allgemein > Einstellungen** definiert sind, werden berücksichtigt.
4. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.
5. Legen Sie mithilfe der Pfeile **↑** und **↓** in der Spalte **Aktion** die Priorität der definierten Update-Server fest. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende **Löschen**-Schaltfläche. Es ist zwar möglich, die standardmäßige Update-Adresse zu entfernen, dies wird jedoch nicht empfohlen.

7.2.11. Exchange-Schutz



Beachten Sie

Dieses Modul steht für Windows for Servers zur Verfügung.

Security for Exchange verfügt über detailliert konfigurierbare Einstellungen, mit denen Microsoft-Exchange-Server gegen Gefahren wie Malware, Spam und Phishing geschützt werden können. Wenn Sie die Software auf Ihrem E-Mail-Server installieren, können Sie entsprechend den Sicherheitsrichtlinien Ihres Unternehmens sowohl Anhänge als auch den Text von E-Mails auf gefährliche Inhalte prüfen.

Um die Leistung des Servers nicht zu beeinträchtigen, verarbeiten die Filter von Security for Exchange den E-Mail-Verkehr in der folgenden Reihenfolge:

1. Spam-Filter
2. Inhaltssteuerung > Inhaltsfilter
3. Inhaltssteuerung > Anhangfilter
4. Malware-Filter

Die Einstellungen für Security for Exchange untergliedern sich in die folgenden Bereiche:

- [Allgemein](#)
- [Malware-Schutz](#)
- [Spam-Schutz](#)
- [Inhalts-Steuerung](#)

Allgemein

In diesem Bereich können Sie Gruppen von E-Mail-Konten erstellen und verwalten, das Alter von Quarantäne-Objekten definieren und bestimmte Absender blockieren.

Benutzergruppen

Im Control Center können Sie Benutzergruppen erstellen, um unterschiedliche Scan- und Filterregeln auf unterschiedliche Benutzerkategorien anzuwenden. Beispielsweise können Sie entsprechende Richtlinien für die IT-Abteilung, die Vertriebsabteilung oder die Manager des Unternehmens erstellen.

Die Benutzergruppen sind unabhängig von der Richtlinie und dem Benutzer, der sie erstellt hat, global verfügbar.

Um die Gruppenverwaltung zu erleichtern, importiert das Control Center die Benutzergruppen automatisch von Windows Active Directory.

So erstellen Sie eine Benutzergruppe:

1. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle. Das Detailfenster wird angezeigt.
2. Geben Sie den Namen und die Beschreibung der Gruppe sowie die E-Mail-Adressen ihrer Benutzer ein.




Beachten Sie

- Wenn die Liste der E-Mail-Adressen sehr lang ist, können Sie sie auch aus einer Textdatei kopieren und einfügen.

- Akzeptierte Trennzeichen sind: Leerzeichen, Komma, Semikolon und Eingabetaste.

3. Klicken Sie auf **Speichern**.

Benutzerdefinierte Gruppen können bearbeitet werden. Wenn Sie auf den Namen der Gruppe klicken, wird ein Konfigurationsfenster angezeigt, in dem Sie Details der Gruppe oder die Benutzerliste ändern können.

Um eine benutzerdefinierte Gruppe aus der Liste zu entfernen, wählen Sie die Gruppen und klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle.



Beachten Sie

Active-Directory-Gruppen können sie weder bearbeiten noch löschen.

Einstellungen

- **Quarantäne-Dateien löschen, die älter sind als (Tage)**. Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Wenn Sie diesen Zeitraum verändern möchten, geben Sie einen anderen Wert in das entsprechende Feld ein.
- **Verbindungs-Blacklist**. Wenn diese Option aktiviert ist, lehnt Exchange Server alle E-Mails von Absendern auf der Blacklist ab.

So erstellen Sie eine Blacklist:

1. Klicken Sie auf den Link **Blacklist-Objekte bearbeiten**.
2. Geben Sie die E-Mail-Adressen ein, die Sie blockieren möchten. Beim Bearbeiten der Liste können Sie zudem Platzhalter verwenden, um ganze E-Mail-Domains oder ein E-Mail-Adressmuster festzulegen:
 - Sternchen (*) ersetzt kein, ein oder mehrere Zeichen.
 - Fragezeichen (?) ersetzt jeden beliebigen Buchstaben.

Wenn Sie zum Beispiel `*@boohouse.com` eingeben, werden alle E-Mail-Adressen unter `boohouse.com` blockiert.

3. Klicken Sie auf **Speichern**.

Domain-IP-Prüfung (Spoofing-Schutz)

Mit diesem Filter verhindern Sie, dass Spammer die E-Mail-Adresse eines vermeintlich vertrauenswürdigen Absenders vortäuschen. Sie können für Ihre

eigene und bei Bedarf auch für andere bekannte E-Mail-Domains die IP-Adressen festlegen, über die ein E-Mail-Versand erfolgen darf. Falls eine E-Mail von einer der aufgeführten Domains zu stammen scheint, die IP-Adresse des Absenders jedoch nicht mit der angegebenen IP-Adresse übereinstimmt, wird die E-Mail abgelehnt.



Warnung

Verwenden Sie diesen Filter nicht, wenn Sie einen Smart Host, einen gehosteten E-Mail-Filterdienst oder eine Gateway-E-Mail-Filterlösung vor Ihren Exchange-Servern einsetzen.



Wichtig

- Dieser Filter überprüft nur nicht authentifizierte E-Mail-Verbindungen.
- Empfohlene Vorgehensweisen:
 - Dieser Filter wird nur für solche Exchange-Server empfohlen, die direkt mit dem Internet verbunden sind. Wenn Sie z. B. sowohl Edge-Transport- als auch Hub-Transport-Server haben, sollten Sie diesen Filter nur auf den Edge-Transport-Servern nutzen.
 - Fügen Sie Ihrer Domain-Liste alle internen IP-Adressen hinzu, die E-Mails über nicht authentifizierte SMTP-Verbindungen senden dürfen. Darunter sind evtl. automatisierte Benachrichtigungssysteme, Netzwerkzubehör wie Drucker, usw.
 - Fügen Sie in einer Exchange-Umgebung mit Datenbankverfügbarkeitsgruppen auch die IP-Adressen aller Ihrer Hub-Transport- und Postfach-Server zu Ihrer Domain-Liste hinzu.
 - Seien Sie vorsichtig bei der Konfiguration von autorisierten IP-Adressen für bestimmte externe E-Mail-Domains, die Sie nicht verwalten. Wenn Sie die Liste der IP-Adressen nicht auf dem neuesten Stand halten, werden die E-Mails von diesen Domains abgelehnt werden. Wenn Sie ein MX-Backup verwenden, müssen Sie allen konfigurierten externen E-Mail-Domains die IP-Adressen hinzufügen, über die MX-Backup E-Mails an Ihre primären Mail-Server sendet.

So konfigurieren Sie den Filter für den Spoofing-Schutz:

1. Wählen Sie die Option **Domain-IP-Prüfung (Spoofing-Schutz)** aus, um den Filter zu aktivieren.
2. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle. Das Konfigurationsfenster wird geöffnet.
3. Geben Sie die E-Mail-Domain in das entsprechende Feld ein.

4. Geben Sie den zulässigen IP-Adressbereich für die im Vorfeld festgelegte Domain im CIDR-Format ein (IP/Netzwerk-Maske).
5. Klicken Sie auf die Schaltfläche **+** **Hinzufügen** auf der rechten Seite der Tabelle. Die IP-Adressen werden der Tabelle hinzugefügt.
6. Um einen IP-Bereich aus der Liste zu entfernen, klicken Sie auf die entsprechende **×** **Löschen**-Schaltfläche auf der rechten Seite der Tabelle.
7. Klicken Sie auf **Speichern**. Die Domain wird dem Filter hinzugefügt.

Sie können eine E-Mail-Domain aus dem Filter entfernen, indem Sie sie in der Spoofing-Schutz-Tabelle auswählen und auf die **−** **Löschen**-Schaltfläche klicken.

Malware-Schutz

Das Malware-Schutz-Modul schützt Exchange-Mail-Server vor einer Vielzahl an Gefahren (Viren, Trojaner, Spyware, Rootkits, Adware, usw.), indem infizierte oder verdächtige Objekte erkannt und desinfiziert oder isoliert werden, je nachdem, welche Aktion in den Einstellungen eingestellt ist.

Malware-Scans werden auf zwei Ebenen durchgeführt:

- **Transport-Ebene**
- **Exchange-Informationsspeicher**

Scan auf der Transportebene

Bitdefender Endpoint Security Tools integriert sich in die E-Mail-Transport-Agenten, um den gesamten E-Mail-Verkehr zu scannen.

Standardmäßig sind Scans der Transport-Ebene aktiviert. Bitdefender Endpoint Security Tools filtert den E-Mail-Datenverkehr und informiert, wenn nötig, den Benutzer im Text der E-Mail selbst über die durchgeführten Aktionen.

Mithilfe des Kästchens **Malware-Filter** können Sie diese Funktion aktivieren und deaktivieren.

Wenn Sie den Benachrichtigungstext ändern möchten, klicken Sie auf den Link **Einstellungen**. Die folgenden Optionen stehen zur Verfügung:

- **Gescannten E-Mails eine Fußzeile hinzufügen.** Markieren Sie dieses Kästchen, wenn Sie möchten, dass unter jede gescannte E-Mail ein Satz eingefügt werden soll. Wenn Sie den Standardtext ändern möchten, können Sie einen anderen Text in das Textfeld darunter eingeben.

- **Ersatztext.** An E-Mails, deren Anhänge gelöscht oder in die Quarantäne verschoben wurden, kann eine Benachrichtigungsdatei angehängt werden. Wenn sie nicht den Standardbenachrichtigungstext verwenden möchten, können Sie in die entsprechenden Textfelder einen eigenen Text eingeben.

Die Malware-Filter basieren auf Regeln. Jede Nachricht, die am Mail-Server ankommt, wird in absteigender Priorität mit den Malware-Filterregeln abgeglichen, bis sie mit einer Regel übereinstimmt. Dann wird die E-Mail gemäß den von dieser Regel festgelegten Optionen verarbeitet.

Filterregeln verwalten

Alle bestehenden Regeln sind, zusammen mit Informationen zu Priorität, Status und Anwendungsbereich, in der Tabelle aufgeführt. Die Regeln sind nach Prioritäten aufgelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste.

Jede Malware-Schutz-Richtlinie hat eine Standardregel, die aktiv wird, sobald die Malware-Filter aktiviert werden. Wissenswertes zur Standardregel:

- Die Regel kann nicht kopiert, deaktiviert oder gelöscht werden.
- Nur die Scan-Einstellungen und Aktionen können geändert werden.
- Die Regel hat immer die niedrigste Priorität.

Regeln erstellen

Sie haben zwei verschiedene Möglichkeiten, Filterregeln zu erstellen:

- Auf den Standardeinstellungen aufbauend; gehen Sie dazu wie folgt vor:
 1. Klicken Sie auf die Schaltfläche **+ Hinzufügen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
 2. Konfigurieren Sie die Regeleinstellungen. Details zu den Optionen hierbei finden Sie unter [Regeloptionen](#).
 3. Klicken Sie auf **Speichern**. Die Regel wird als erste in der Tabelle aufgeführt.
- Auf der Grundlage eines Klons einer benutzerdefinierten Regel; gehen Sie dazu wie folgt vor:
 1. Wählen Sie die gewünschte Regel aus der Tabelle.
 2. Klicken Sie auf die Schaltfläche **🔄 Klonen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
 3. Passen Sie die Regeloptionen nach Bedarf an.
 4. Klicken Sie auf **Speichern**. Die Regel wird als erste in der Tabelle aufgeführt.



Regeln bearbeiten

So bearbeiten Sie eine bestehende Regel:

1. Klicken Sie auf den Namen der Regel, um das Konfigurationsfenster zu öffnen.
2. Geben Sie neue Werte für die Optionen ein, die Sie ändern möchten.
3. Klicken Sie auf **Speichern**. Die Änderungen greifen, sobald die Richtlinie gespeichert wird.


Regelpriorität festlegen

So ändern Sie die Priorität einer Regel:

1. Wählen Sie die gewünschte Regel.
2. Mithilfe der Schaltflächen  **Hoch** und  **Runter** am oberen Rand der Tabelle können Sie die Priorität der Regel erhöhen bzw. verringern.

Regeln entfernen

Benutzerdefinierte Regeln können Sie einzeln oder als Gruppe löschen. Gehen Sie dazu wie folgt vor:

1. Markieren Sie die Kästchen, der Regeln, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle. Eine gelöschte Regel kann nicht wiederhergestellt werden.

Regeloptionen

Die folgenden Optionen stehen zur Verfügung:

- **Allgemein**. In diesem Bereich muss ein Name für die Regel eingegeben werden. Sonst kann sie nicht gespeichert werden. Markieren Sie das Kästchen **Aktiv**, wenn sie möchten, dass die Regel gilt, sobald die Richtlinie gespeichert wird.
- **Regel-Anwendungsbereich**. Sie können den Anwendungsbereich einer Regel einschränken, sodass sie nur auf bestimmte E-Mails angewendet wird. Dazu können Sie die folgenden kumulativen Optionen verwenden:
 - **Anwenden auf (Richtung)**. Wählen Sie die Richtung des E-Mail-Datenverkehrs, für die die Regel gelten soll.
 - **Absender**. Hier können Sie einstellen, ob die Regel für alle oder nur für bestimmte Absender gelten soll. Um die Anzahl der Absender einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.
 - **Empfänger**. Hier können Sie festlegen, ob die Regel für alle oder nur für bestimmte Empfänger gelten soll. Um die Anzahl der Empfänger einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.

Die Regel wird angewendet, wenn mindestens ein von Ihnen ausgewählter Empfänger dabei ist. Wenn Sie die Regeln nur anwenden möchten, wenn alle Empfänger in der ausgewählten Gruppe sind, wählen Sie **Alle Empfänger abgleichen**.



Beachten Sie

Die Adressen in den Feldern **Cc** und **Bcc** werden auch als Empfänger angesehen.



Wichtig

Regeln, die auf Benutzergruppen basieren, gelten nur für die Rollen Hub-Transport und Postfach.

- **Optionen.** Hier können Sie die Scan-Optionen für E-Mails einstellen, die zu einer Regel passen:
 - **Gesamte Dateitypen.** Mit dieser Option legen Sie fest, welche Dateitypen gescannt werden. Sie können einstellen, dass alle Dateien gescannt werden (unabhängig von der Dateierweiterung), nur Anwendungsdateien oder nur bestimmte Dateierweiterungen, die Sie für gefährlich halten. Das Scannen aller Dateien bietet den besten Schutz, nur Anwendungsdateien zu scannen ist schneller.



Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter [„Anwendungsdateitypen“](#) (S. 545).

Wenn Sie nur Dateien mit bestimmten Erweiterungen scannen möchten, haben Sie zwei Möglichkeiten:

- **Benutzerdefinierte Erweiterungen;** geben Sie hier nur die Erweiterungen der Dateitypen ein, die gescannt werden sollen.
- **Alle Dateien außer bestimmten Erweiterungen;** hierbei geben sie nur die Dateierweiterungen ein, die nicht gescannt werden sollen.
- **Maximalgröße für Anhang/Nachrichteninhalte (in MB).** Markieren Sie dieses Kästchen und geben Sie einen Wert in das entsprechende Feld ein, um die Maximalgröße für angehängte Dateien oder Nachrichteninhalte festzulegen, bis zu der gescannt werden soll.
- **Maximale Archivtiefe (Ebenen).** Markieren Sie dieses Kästchen und wählen Sie die maximale Archivtiefe im entsprechenden Feld. Je geringer dieser Wert, desto höher die Leistung und geringer die Sicherheit.

- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Markieren Sie dieses Kästchen, um nach potenziell böartigen oder unerwünschten Anwendungen zu scannen, z. B. Adware, die sich ohne Zustimmung des Benutzers auf dem System installiert, das Verhalten anderer Software beeinflusst oder die Systemleistung einschränkt.
- **Aktionen.** Sie können für den Sicherheitsagenten abhängig von der Erkennungsart verschiedene automatische Aktionen für Dateien festlegen.

Über die Erkennungsart werden Dateien in drei Kategorien unterteilt:

- **Infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI).
- **Verdächtige Dateien.** Diese Dateien werden durch heuristische Analyse und andere Bitdefender-Technologien als verdächtig eingestuft. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden).
- **Unscanbare Dateien.** Diese Dateien können nicht gescannt werden. So können zum Beispiel passwortgeschützte, verschlüsselte oder überkomprimierte Dateien nicht gescannt werden.

Für jeden Erkennungstyp gibt es eine Standard- oder Hauptaktion und eine alternative Aktion für den Fall, dass die Hauptaktion fehlschlägt. Es wird nicht empfohlen, aber wenn Sie möchten, können Sie diese Aktionen über die entsprechenden Menüs ändern. Wählen Sie die Aktion, die ausgeführt werden soll:

- **Desinfizieren.** Entfernt den schädlichen Code aus infizierten Dateien und rekonstruiert die Originaldatei. Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
- **E-Mail ablehnen/löschen.** Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei löschen.** Entfernt problematische Anhänge ohne Warnung. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei ersetzen.** Entfernt problematische Dateien und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert.

- **Datei in die Quarantäne verschieben.** verschiebt erkannte Dateien in den Quarantäneordner und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. In die Quarantäne verschobene Dateien können Sie auf der Seite **Quarantäne** verwalten.




Beachten Sie

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist. Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

- **Keine Aktion durchführen.** Wenn problematische Dateien gefunden werden, wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen. Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.
- Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden.**

Ausschlüsse

Wenn Sie möchten, dass bestimmte E-Mails nicht gefiltert werden, können Sie dazu Scan-Ausschlüsse definieren. So erstellen Sie einen Ausschluss:

1. Erweitern Sie den Bereich **Ausschlüsse für Malware-Schutz-Regeln**.
2. Klicken Sie in der Symbolleiste dieses Bereichs auf die Schaltfläche  **Hinzufügen**. Das Konfigurationsfenster wird angezeigt.
3. Konfigurieren Sie die Einstellungen für den Ausschluss. Details zu den Optionen hierbei finden Sie unter [Regeloptionen](#).
4. Klicken Sie auf **Speichern**.

Scannen des Exchange-Informationsspeichers

Der Exchange-Schutz setzt Exchange Web Services (EWS) von Microsoft ein, um die Datenbanken der Exchange-Postfächer und der öffentlichen Ordner scannen zu können. Sie können das Malware-Schutz-Modul so konfigurieren, dass die

gewünschten Datenbanken in von Ihnen festgelegten Abständen gescannt werden (Bedarf-Scans).

Beachten Sie

- Bedarf-Scans sind nur für Exchange-Server mit Postfach-Rolle verfügbar.
- Beachten Sie hierbei, dass Bedarf-Scans ressourcenintensiv sind und, je nach eingestellten Scan-Optionen und Anzahl der zu scannenden Objekte, einige Zeit dauern können.

Für Bedarf-Scans wird ein Exchange-Administrator-Konto (Dienstkonto) benötigt, um die Identität von Exchange-Benutzern annehmen zu können und die zu scannenden Objekte aus den Benutzer-Postfächern und öffentlichen Ordnern abzurufen. Es wird empfohlen, hierfür ein eigenes Konto einzurichten.

Das Exchange-Administratorkonto muss die folgenden Voraussetzungen erfüllen:

- Es handelt sich dabei um ein Mitglied der Gruppe Organisationsverwaltung (Exchange 2013 und 2010)
- Es ist ein Mitglied der Gruppe Exchange-Organisationsadministratoren (Exchange 2007)
- Es hat ein Postfach.

Bedarf-Scans aktivieren

1. Klicken Sie im Bereich **Scan-Aufgaben** auf den Link **Zugangsdaten hinzufügen**.
2. Geben Sie den Benutzernamen und das Passwort für das Dienstkonto ein.
3. Wenn die E-Mail-Adresse nicht der Benutzername ist, müssen Sie auch die E-Mail-Adresse des Dienstkontos eingeben.
4. Geben Sie die URL für Exchange Web Services (EWS) ein. Sie wird benötigt, falls die Exchange-AutoErmittlung nicht funktioniert.


Beachten Sie

- Der Benutzername muss den Domain-Namen enthalten, z. B. `Benutzer@Domain` oder `Domain\Benutzer`.
- Denken Sie daran, die Zugangsdaten im Control Center zu aktualisieren, nachdem sie geändert wurden.


Scan-Aufgaben verwalten

In der Scan-Aufgaben-Tabelle werden alle geplanten Aufgaben mit den zugehörigen Zielen und Wiederholungsintervallen angezeigt.

So erstellen Sie Aufgaben für Scans des Exchange-Informationsspeichers:

1. Klicken Sie im Bereich **Scan-Aufgaben** auf die Schaltfläche  **Hinzufügen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
2. Konfigurieren Sie die Aufgaben-Einstellungen, wie dort beschrieben.
3. Klicken Sie auf **Speichern**. Die Aufgabe wird der Liste hinzugefügt und greift, sobald die Richtlinie gespeichert wird.

Sie können Aufgaben jederzeit bearbeiten, indem Sie einfach auf den Aufgabennamen klicken.

Um Aufgaben aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle.

Scan-Aufgaben-Einstellungen

Für Aufgaben stehen die folgenden Einstellungen zur Verfügung:

- **Allgemein.** Geben Sie einen aussagekräftigen Namen für die Aufgabe ein.



Beachten Sie

Der Name der Aufgabe wird in der Zeitleiste von Bitdefender Endpoint Security Tools aufgeführt.

- **Planer.** Verwenden Sie die Planungsoptionen, um den Scan-Zeitplan zu konfigurieren. Sie können festlegen, dass der Scan alle paar Stunden, Tage oder Wochen durchgeführt wird und Datum und Zeit des ersten Scans bestimmen. Bei großen Datenbanken kann der Scan lange dauern und die Serverleistung beeinträchtigen. In solchen Fällen können Sie einstellen, dass die Scan-Aufgabe nach einer bestimmten Zeit angehalten wird.
- **Ziel.** Hier können Sie Container und Objekte auswählen, die gescannt werden sollen. Sie können Postfächer, öffentliche Ordner oder beides scannen lassen. Außer E-Mails können Sie auch andere Objekte wie **Kontakte, Aufgaben, Termine** und **Mail-Objekte** scannen lassen. Außerdem können Sie den Scan wie folgt einschränken:
 - Nur ungelesene E-Mails
 - Nur Objekte mit Anhängen
 - Nur neue Objekte, die in einem bestimmten Zeitraum empfangen wurden

So können Sie zum Beispiel nur E-Mails in Benutzer-Postfächern scannen lassen, die in den letzten sieben Tagen empfangen wurden.

Markieren Sie das Kästchen **Ausschlüsse**, wenn Sie Scan-Ausnahmen definieren möchten. So erstellen Sie mithilfe der Felder in der Tabellenüberschrift eine Ausnahme:

1. Wählen Sie den Repository-Typ aus dem Menü.
2. Geben Sie je nach Repository-Typ das auszuschließende Objekt an:

Repository-Typ	Objektformat
Postfach	E-Mail-Adresse
Öffentlicher Ordner	Ordnerpfad, von Root ausgehend
Datenbank	Die Datenbankidentität



Beachten Sie

Mit dem folgenden Exchange-Shell-Befehl können Sie die Datenbankidentität abrufen:

```
Get-MailboxDatabase | fl name,identity
```

Sie können nicht mehr als ein Objekt gleichzeitig eingeben. Wenn Sie mehrere Objekte desselben Typs haben, müssen Sie für jedes einzelne Objekt eine eigene Regel definieren.

3. Klicken Sie am oberen Rand der Tabelle auf die Schaltfläche **+ Hinzufügen**, um die Ausnahme zu speichern und der Liste hinzuzufügen.

Um eine Ausnahmenregel aus der Liste zu löschen, klicken Sie auf die entsprechende **- Löschen**-Schaltfläche.

- **Optionen.** Hier können Sie die Scan-Optionen für E-Mails einstellen, die zu einer Regel passen:
 - **Gesamte Dateitypen.** Mit dieser Option legen Sie fest, welche Dateitypen gescannt werden. Sie können einstellen, dass alle Dateien gescannt werden (unabhängig von der Dateierstreckung), nur Anwendungsdateien oder nur bestimmte Dateierstreckungen, die Sie für gefährlich halten. Das Scannen aller Dateien bietet den besten Schutz, nur Anwendungsdateien zu scannen ist schneller.



Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „[Anwendungsdateitypen](#)“ (S. 545).

Wenn Sie nur Dateien mit bestimmten Endungen scannen möchten, haben Sie zwei Möglichkeiten:

- **Benutzerdefinierte Endungen;** geben Sie hier nur die Endungen der Dateitypen ein, die gescannt werden sollen.
- **Alle Dateien außer bestimmten Endungen;** hierbei geben sie nur die Dateiendungen ein, die nicht gescannt werden sollen.
- **Maximalgröße für Anhang/Nachrichteninhalt (in MB).** Markieren Sie dieses Kästchen und geben Sie einen Wert in das entsprechende Feld ein, um die Maximalgröße für angehängte Dateien oder Nachrichteninhalte festzulegen, bis zu der gescannt werden soll.
- **Maximale Archivtiefe (Ebenen).** Markieren Sie dieses Kästchen und wählen Sie die maximale Archivtiefe im entsprechenden Feld. Je geringer dieser Wert, desto höher die Leistung und geringer die Sicherheit.
- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Markieren Sie dieses Kästchen, um nach potenziell böartigen oder unerwünschten Anwendungen zu scannen, z. B. Adware, die sich ohne Zustimmung des Benutzers auf dem System installiert, das Verhalten anderer Software beeinflusst oder die Systemleistung einschränkt.
- **Aktionen.** Sie können für den Sicherheitsagenten abhängig von der Erkennungsart verschiedene automatische Aktionen für Dateien festlegen.

Über die Erkennungsart werden Dateien in drei Kategorien unterteilt:

- **Infizierte Dateien.** Bitdefender nutzt verschiedene ausgefeilte Mechanismen, um infizierte Dateien als solche zu erkennen, darunter Malware-Signaturen, Maschinelles Lernen und künstliche Intelligenz (KI).
- **Verdächtige Dateien.** Diese Dateien werden durch heuristische Analyse und andere Bitdefender-Technologien als verdächtig eingestuft. Dadurch kommt eine hohe Erkennungsrate zustande, allerdings kommt es gelegentlich auch zu falschpositiven Ergebnissen (unbedenkliche Dateien, die als verdächtig eingestuft werden).
- **Unscanbare Dateien.** Diese Dateien können nicht gescannt werden. So können zum Beispiel passwortgeschützte, verschlüsselte oder überkomprimierte Dateien nicht gescannt werden.

Für jeden Erkennungstyp gibt es eine Standard- oder Hauptaktion und eine alternative Aktion für den Fall, dass die Hauptaktion fehlschlägt. Es wird nicht empfohlen, aber wenn Sie möchten, können Sie diese Aktionen über die entsprechenden Menüs ändern. Wählen Sie die Aktion, die ausgeführt werden soll:

- **Desinfizieren.** Entfernt den schädlichen Code aus infizierten Dateien und rekonstruiert die Originaldatei. Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
- **E-Mail ablehnen/löschen.** Die E-Mail wird ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei löschen.** Entfernt problematische Anhänge ohne Warnung. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **Datei ersetzen.** Entfernt problematische Dateien und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert.
- **Datei in die Quarantäne verschieben.** verschiebt erkannte Dateien in den Quarantäneordner und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. In die Quarantäne verschobene Dateien können Sie auf der Seite **Quarantäne** verwalten.



Beachten Sie

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist. Die Größe der Quarantäne hängt von der Anzahl und Größe der darin gespeicherten E-Mails ab.

- **Keine Aktion durchführen.** Wenn problematische Dateien gefunden werden, wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen. Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtige Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.
- Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden.**

Spam-Schutz

Das Spam-Schutz-Modul bietet durch den Einsatz verschiedener Filter und Engines mehrschichtige Sicherheit vor Spam und Phishing.

Beachten Sie

- Spam-Filter stehen zur Verfügung für:
 - Exchange Server 2016/2013 mit Edge-Transport- oder Postfach-Rolle
 - Exchange Server 2010/2007 mit Edge-Transport- oder Hub-Transport-Rolle
- Wenn Sie in Ihrer Exchange-Struktur sowohl Edge- als auch Hub-Rollen haben, empfehlen wir die Spam-Filter auf dem Server mit der Edge-Transport-Rolle zu aktivieren.

Für eingehende E-Mails sind die Spam-Filter automatisch aktiviert. Mithilfe des Kästchens **Spam-Filter** können Sie diese Funktion deaktivieren und wieder aktivieren.

Spam-Filter

Jede E-Mail wird auf der Grundlage von Absender- und Empfängergruppe mit den Spam-Filter-Regeln in absteigender Priorität verglichen, bis sie mit einer Regel übereinstimmt. Die E-Mail wird dann gemäß der Regeloptionen verarbeitet, und entsprechende Aktionen werden für gefundenen Spam durchgeführt.

Einige Spam-Filter können konfiguriert werden und ein- oder ausgeschaltet werden. Im Folgenden werden alle optionalen Filter beschrieben:

- **Zeichensatz-Filter.** viele Spam-E-Mails sind in kyrillischen oder asiatischen Zeichensätzen verfasst. Der Zeichensatz-Filter erkennt diese Art von E-Mails und markiert sie als SPAM.
- **Sexuelle Inhalte.** Spam mit sexuellen Inhalten muss den Warnhinweis SEXUELLE INHALTE im Betreff beinhalten. Dieser Filter erkennt E-Mails, die im Betreff als E-Mail mit sexuellem Inhalt markiert wurden, und markiert diese als SPAM.
- **URL-Filter.** Fast alle Spam-Mails enthalten Links zu verschiedenen Webseiten. Meist finden sich auf den entsprechenden Webseiten Werbung und andere Kaufanreize. Manchmal werden sie auch zum Phishing eingesetzt.

Bitdefender unterhält eine Datenbank dieser Links, die ständig aktualisiert wird. Der URL-Filter gleicht jeden in einer E-Mail enthaltenen URL-Link mit dieser Datenbank ab. Wird eine Übereinstimmung gefunden, wird die E-Mail als Spam markiert.

- **Realtme Blackhole List (RBL).** Hierbei handelt es sich um einen Filter, durch den der Mail-Server des Absenders in Echtzeit mit einer von Dritten betriebenen Liste verdächtiger Server abgeglichen wird. Der Filter verwendet das DNSBL-Protokoll und die RBL-Server, um Spam auf der Grundlage der Einstufung des Mail-Servers als Spam-Quelle zu filtern.

Die Mail-Server-Adresse wird dem E-Mail-Header entnommen und auf ihre Gültigkeit hin überprüft. Wenn die Adresse zu einer privaten Klasse gehört (10.0.0.0, 172.16.0.0 bis 172.31.0.0 oder 192.168.0.0 bis 192.168.255.0), wird sie ignoriert.

Eine DNS-Prüfung wird für die Domain `d.c.b.a.rbl.example.com` durchgeführt, bei der `d.c.b.a` die umgekehrte IP-Adresse des Servers ist und `rbl.example.com` der RBL-Server ist. Wenn das DNS antwortet, dass die Domain gültig ist, bedeutet dies, dass die IP-Adresse im RBL-Server aufgelistet ist. Dann wird eine Einstufung (Server Score) vergeben. Diese Einstufung wird mit einem Wert zwischen 0 und 100 dargestellt, je nachdem, wie sehr diesem Server vertraut wird.

Die für jeden der in der Liste aufgeführten RBL-Server durchgeführte Abfrage und die von jedem erhaltene Einstufung wird zur mittelfristigen Einstufung addiert. Wenn der Wert 100 erreicht, werden keine weiteren Abfragen durchgeführt.

Wenn der RBL-Filter-Wert 100 oder mehr beträgt, wird die E-Mail als Spam eingestuft und eine entsprechende Aktion durchgeführt. Andernfalls wird eine Spam-Einstufung auf der Grundlage des RBL-Filter-Werts berechnet und zur Gesamt-Spam-Einstufung der E-Mail addiert.

- **Heuristische Filter.** Der von Bitdefender entwickelte heuristische Filter erkennt neuen und unbekanntes Spam. Dieser Filter wird automatisch mit großen Mengen von Spam-E-Mails aus den Bitdefender-Spam-Labors gefüttert. Dabei „lernt“ er zwischen Spam und legitimen E-Mails zu unterscheiden und kann so neuen Spam durch, oft sehr unauffällige, Ähnlichkeiten mit den zuvor gefütterten Spam-E-Mails erkennen. Dieser Filter ist so konzipiert, dass die Signatur-basierte Erkennung verbessert und gleichzeitig die Anzahl der Falschmeldungen so gering wie möglich gehalten wird.
- **Bitdefender-Cloud-Abfrage.** Bitdefender unterhält eine ständig wachsende Datenbank von "Spam-E-Mail-Fingerabdrücken" in der Cloud. Eine Abfrage mit dem Fingerabdruck der E-Mail wird an die Server in der Cloud gesendet, um augenblicklich zu prüfen, ob die E-Mail Spam ist. Auch wenn der Fingerabdruck

selbst nicht in der Datenbank vorhanden ist, wird er mit anderen Abfragen aus der letzten Zeit verglichen, und die E-Mail kann dann, sofern bestimmte Bedingungen erfüllt sind, als Spam markiert werden.

Spam-Schutz-Regeln verwalten

Alle bestehenden Regeln sind, zusammen mit Informationen zu Priorität, Status und Anwendungsbereich, in der Tabelle aufgeführt. Die Regeln sind nach Prioritäten aufgelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste.

Jede Spam-Schutz-Richtlinie hat eine Standardregel, die aktiv wird, sobald das Modul aktiviert wird. Wissenswertes zur Standardregel:

- Die Regel kann nicht kopiert, deaktiviert oder gelöscht werden.
- Nur die Scan-Einstellungen und Aktionen können geändert werden.
- Die Regel hat immer die niedrigste Priorität.

Regeln erstellen

Um eine Regel anzulegen:

1. Klicken Sie auf die Schaltfläche **+** **Hinzufügen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
2. Konfigurieren Sie die Regeleinstellungen. Weitere Details zu den Optionen finden Sie unter „[Regeloptionen](#)“ (S. 386)
3. Klicken Sie auf **Speichern**. Die Regel wird als erste in der Tabelle aufgeführt.

Regeln bearbeiten

So bearbeiten Sie eine bestehende Regel:

1. Klicken Sie auf den Namen der Regel, um das Konfigurationsfenster zu öffnen.
2. Geben Sie neue Werte für die Optionen ein, die Sie ändern möchten.
3. Klicken Sie auf **Speichern**. Wenn die Regel aktiv ist, greifen die Änderungen, sobald die Richtlinie gespeichert wird.

Regelpriorität festlegen

Wenn Sie die Priorität einer Regel ändern möchten, wählen Sie die entsprechende Regel aus, und schieben Sie sie mithilfe der Pfeile **⬆ Hoch** und **⬇ Runter** am oberen Rand der Tabelle an die gewünschte Position. Sie können nicht mehr als eine Regel gleichzeitig verschieben.

Regeln entfernen

Wenn Sie eine bestimmte Regel nicht mehr verwenden möchten, wählen Sie sie aus und klicken Sie dann am oberen Rand der Tabelle auf die Schaltfläche **⊖ Löschen**.

Regeloptionen

Die folgenden Optionen stehen zur Verfügung:

- **Allgemein.** In diesem Bereich muss ein Name für die Regel eingegeben werden. Sonst kann sie nicht gespeichert werden. Markieren Sie das Kästchen **Aktiv**, wenn sie möchten, dass die Regel gilt, sobald die Richtlinie gespeichert wird.
- **Regel-Anwendungsbereich.** Sie können den Anwendungsbereich einer Regel einschränken, sodass sie nur auf bestimmte E-Mails angewendet wird. Dazu können Sie die folgenden kumulativen Optionen verwenden:
 - **Anwenden auf (Richtung).** Wählen Sie die Richtung des E-Mail-Datenverkehrs, für die die Regel gelten soll.
 - **Absender.** Hier können Sie einstellen, ob die Regel für alle oder nur für bestimmte Absender gelten soll. Um die Anzahl der Absender einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.
 - **Empfänger.** Hier können Sie festlegen, ob die Regel für alle oder nur für bestimmte Empfänger gelten soll. Um die Anzahl der Empfänger einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.

Die Regel wird angewendet, wenn mindestens ein von Ihnen ausgewählter Empfänger dabei ist. Wenn Sie die Regeln nur anwenden möchten, wenn alle Empfänger in der ausgewählten Gruppe sind, wählen Sie **Alle Empfänger abgleichen**.



Beachten Sie

Die Adressen in den Feldern **Cc** und **Bcc** werden auch als Empfänger angesehen.



Wichtig

Regeln, die auf Benutzergruppen basieren, gelten nur für die Rollen Hub-Transport und Postfach.

- **Einstellungen.** Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (**aggressiv**, **normal** oder **tolerant**). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Zusätzlich können Sie verschiedene Filter aktivieren. Detaillierte Informationen zu diesen Filtern finden Sie unter „Spam-Filter“ (S. 383).



Wichtig

Für den RBL-Filter ist weitergehende Konfiguration nötig. Sie können diese Konfiguration vornehmen, nachdem Sie die Regel erstellt oder bearbeitet haben. Weitere Informationen finden Sie unter „[Den RBL-Filter konfigurieren](#)“ (S. 388)

Für authentifizierte Verbindungen können Sie einstellen, dass die Spam-Filterung umgangen wird.

- **Aktionen.** Für als Spam markierte E-Mails können Sie verschiedene Aktionen durchführen. Jede dieser Aktionen hat wiederum verschiedene Optionen und/oder sekundäre Aktionen. Sie werden im Folgenden beschrieben:

Hauptaktionen:

- **E-Mail zustellen.** Die Spam-E-Mail wird den Postfächern der Empfänger zugestellt.
- **E-Mail in die Quarantäne verschieben.** Die E-Mail wird verschlüsselt und im Quarantäne-Ordner des Exchange-Servers gespeichert; sie wird nicht den Empfängern zugestellt. In die Quarantäne verschobene E-Mails können Sie auf der Seite **Quarantäne** verwalten.
- **E-Mail umleiten an.** Die E-Mail wird nicht den ursprünglichen Empfängern zugestellt, sondern einem Postfach, das Sie im entsprechenden Feld angeben können.
- **E-Mail ablehnen/löschen.** Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Sekundäre Aktionen:

- **Mit Exchange SCL integrieren.** Fügt der Spam-E-Mail einen Header hinzu, wodurch der Exchange-Server oder Microsoft Outlook eine Aktion gemäß dem SCL-Mechanismus durchführen kann.
- **E-Mail-Betreff markieren als.** Sie können dem E-Mail-Betreff eine Bezeichnung hinzufügen, damit andere Benutzer die E-Mail in ihrem Mail-Client filtern können.
- **E-Mail-Header hinzufügen.** Den als Spam erkannten E-Mails wird ein Header hinzugefügt. Sie können den Namen und Wert dieses Headers ändern, indem Sie den gewünschten Informationen in die entsprechenden Felder eingeben. Später können Sie diesen E-Mail-Header verwenden, um zusätzliche Filter zu erstellen.

- **E-Mail auf der Festplatte speichern.** Eine Kopie der Spam-E-Mail wird als Datei im angegebenen Ordner gespeichert. Geben Sie den absoluten Pfad des Ordners in das entsprechende Feld ein.



Beachten Sie

Diese Option funktioniert nur mit E-Mails im MIME-Format.

- **Im Konto archivieren.** Eine Kopie der erkannten E-Mail wird an die angegebene E-Mail-Adresse gesendet. Mit dieser Aktion wird die E-Mail-Adresse der Blindkopie-Liste (Bcc-Liste) hinzugefügt.
- Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden**.

Den RBL-Filter konfigurieren

Wenn Sie den **RBL-Filter** verwenden möchten, müssen Sie eine Liste mit RBL-Servern anlegen.

So konfigurieren Sie den Filter:

1. Klicken Sie auf der Seite **Spam-Schutz** auf den Link **Einstellungen**, um das Konfigurationsfenster zu öffnen.
2. Geben Sie die IP-Adresse des abzufragenden DNS-Servers und das Abfrage-Timeout-Intervall in die entsprechenden Felder ein. Wenn keine DNS-Serveradresse konfiguriert wurde oder der DNS-Server nicht verfügbar ist, verwendet der RBL-Filter die DNS-Server des Systems.
3. Gehen Sie für jeden RBL-Server wie folgt vor:
 - a. Geben Sie den Hostnamen oder die IP-Adresse des Servers und den Confidence Level, den Sie diesem Server gegeben haben, in die Felder der Tabellenüberschrift ein.
 - b. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle.
4. Klicken Sie auf **Speichern**.

Absender-Whitelist konfigurieren

Sie können Server-Ressourcen sparen, indem Sie bekannte Absender auf die Liste vertrauenswürdiger (Whitelist) oder nicht vertrauenswürdiger (Blacklist) Absender setzen. Damit wird der Mail-Server E-Mails von diesen Absendern immer akzeptieren bzw. ablehnen. Wenn Sie zum Beispiel regen E-Mail-Verkehr mit einem

Geschäftspartner haben und sicherstellen möchten, dass Sie keine seiner E-Mails verpassen, können Sie seine E-Mail-Adresse auf die Whitelist setzen.

So erstellen Sie eine Whitelist vertrauenswürdiger Absender:

1. Klicken Sie auf den Link **Whitelist**, um das Konfigurationsfenster zu öffnen.
2. Markieren Sie das Kästchen **Absender-Whitelist**.
3. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein. Beim Bearbeiten der Liste können Sie zudem Platzhalter verwenden, um ganze E-Mail-Domains oder ein E-Mail-Adressmuster festzulegen:

- Sternchen (*) ersetzt kein, ein oder mehrere Zeichen.
- Fragezeichen (?) ersetzt jeden beliebigen Buchstaben.

Wenn Sie zum Beispiel *.gov eingeben, werden alle eingehenden E-Mails akzeptiert, die über eine .gov-Domain versendet wurden.

4. Klicken Sie auf **Speichern**.



Beachten Sie

Bekannte Spam-Versender können Sie auf die Blacklist setzen, indem Sie im Bereich **Exchange-Schutz > Allgemein > Einstellungen** die Option **Blacklist für Verbindungen** verwenden.

Inhalts-Steuerung

Mit der Inhaltssteuerung können Sie die E-Mail-Sicherheit weiter erhöhen, indem Sie allen E-Mail-Verkehr, der gegen Ihre Unternehmensrichtlinien verstößt (unerwünschte oder vertrauliche Inhalte) filtern.

Das Modul enthält zwei Filtermöglichkeiten:

- [Inhaltsfilterung](#)
- [Anhangsfilterung](#)



Beachten Sie

Inhalts- und an Anhangsfilterung stehen zur Verfügung für:

- Exchange Server 2016/2013 mit Edge-Transport- oder Postfach-Rolle
- Exchange Server 2010/2007 mit Edge-Transport- oder Hub-Transport-Rolle

Filterregeln verwalten

Die Filter der Inhaltssteuerung basieren auf Regeln. Sie können verschiedene Regeln für unterschiedliche Benutzer und Benutzergruppen erstellen. Jede E-Mail, die am

Mail-Server ankommt, wird in absteigender Priorität mit den Filterregeln abgeglichen, bis sie mit einer Regel übereinstimmt. Dann wird die E-Mail gemäß den von dieser Regel festgelegten Optionen verarbeitet.

Die Inhaltsfilterungsregeln haben Vorrang vor den Anhangsfilterungsregeln.

Inhalts- und Anhangsfilterregeln sind in den jeweiligen Tabellen nach Priorität geordnet aufgeführt; die erste Regel hat dabei immer die höchste Priorität. Für jede Regel werden die folgenden Informationen angezeigt:

- Priorität
- Name
- Datenverkehrsrichtung
- Absender- und Empfängergruppen

Regeln erstellen

Sie haben zwei verschiedene Möglichkeiten, Filterregeln zu erstellen:

- Auf den Standardeinstellungen aufbauend; gehen Sie dazu wie folgt vor:
 1. Klicken Sie auf die Schaltfläche **+** **Hinzufügen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
 2. Konfigurieren Sie die Regeleinstellungen. Details zu den einzelnen Inhalts- und Anhangsfiltermöglichkeiten finden Sie hier:
 - [Regeloptionen für die Inhaltsfilterung](#)
 - [Regeloptionen für Anhangsfilter](#).
 3. Klicken Sie auf **Speichern**. Die Regel wird als erste in der Tabelle aufgeführt.
- Auf der Grundlage eines Klons einer benutzerdefinierten Regel; gehen Sie dazu wie folgt vor:
 1. Wählen Sie die gewünschte Regel aus der Tabelle.
 2. Klicken Sie auf die Schaltfläche **+** **Klonen** am oberen Rand der Tabelle. Das Konfigurationsfenster wird angezeigt.
 3. Passen Sie die Regeloptionen nach Bedarf an.
 4. Klicken Sie auf **Speichern**. Die Regel wird als erste in der Tabelle aufgeführt.



Regeln bearbeiten

So bearbeiten Sie eine bestehende Regel:

1. Klicken Sie auf den Namen der Regel, um das Konfigurationsfenster zu öffnen.
2. Geben Sie neue Werte für die Optionen ein, die Sie ändern möchten.
3. Klicken Sie auf **Speichern**. Die Änderungen greifen, sobald die Richtlinie gespeichert wird.


Regelpriorität festlegen

So ändern Sie die Priorität einer Regel:

1. Wählen Sie die gewünschte Regel.
2. Mithilfe der Schaltflächen  **Hoch** und  **Runter** am oberen Rand der Tabelle können Sie die Priorität der Regel erhöhen bzw. verringern.

Regeln entfernen

Sie können beliebig viele benutzerdefinierte Regeln löschen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie die Regeln, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle. Eine gelöschte Regel kann nicht wiederhergestellt werden.

Inhaltsfilterung

Mit Inhaltsfiltern können Sie E-Mails nach bestimmten Zeichenfolgen filtern. Diese Zeichenfolgen werden mit dem Betreff oder mit dem Nachrichteninhalte verglichen. Durch die Anwendung von Inhaltsfilterung, können Sie folgendes erreichen:

- Verhindern, dass unerwünschte E-Mail-Inhalte in die Exchange-Server-Postfächer gelangen.
- Verhindern, dass E-Mails mit vertraulichen Daten nach außen gelangen.
- E-Mails, die bestimmte Bedingungen erfüllen, in einem anderen E-Mail-Konto oder auf einem anderen Medium speichern. Sie können z. B. E-Mails, die an die Support-Adresse Ihres Unternehmens geschickt werden, in einem eigenen Ordner auf der Festplatte speichern.

Inhaltsfilterung aktivieren

Wenn Sie die Inhaltsfilterung verwenden möchten, markieren Sie das Kästchen **Inhaltsfilterung**.

Wie Sie Regeln für die Inhaltsfilterung erstellen und verwalten erfahren Sie unter [„Filterregeln verwalten“](#) (S. 389).

Regeloptionen

- **Allgemein.** In diesem Bereich muss ein Name für die Regel eingegeben werden. Sonst kann sie nicht gespeichert werden. Markieren Sie das Kästchen **Aktiv**, wenn sie möchten, dass die Regel gilt, sobald die Richtlinie gespeichert wird.
- **Regel-Anwendungsbereich.** Sie können den Anwendungsbereich einer Regel einschränken, sodass sie nur auf bestimmte E-Mails angewendet wird. Dazu können Sie die folgenden kumulativen Optionen verwenden:

- **Anwenden auf (Richtung).** Wählen Sie die Richtung des E-Mail-Datenverkehrs, für die die Regel gelten soll.
- **Absender.** Hier können Sie einstellen, ob die Regel für alle oder nur für bestimmte Absender gelten soll. Um die Anzahl der Absender einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.
- **Empfänger.** Hier können Sie festlegen, ob die Regel für alle oder nur für bestimmte Empfänger gelten soll. Um die Anzahl der Empfänger einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.

Die Regel wird angewendet, wenn mindestens ein von Ihnen ausgewählter Empfänger dabei ist. Wenn Sie die Regeln nur anwenden möchten, wenn alle Empfänger in der ausgewählten Gruppe sind, wählen Sie **Alle Empfänger abgleichen**.



Beachten Sie

Die Adressen in den Feldern **Cc** und **Bcc** werden auch als Empfänger angesehen.



Wichtig

Regeln, die auf Benutzergruppen basieren, gelten nur für die Rollen Hub-Transport und Postfach.

- **Einstellungen.** Hier können Sie die Zeichenfolgen definieren, nach denen in E-Mails gesucht werden soll. Gehen Sie dazu wie folgt vor:
 1. Wählen Sie, in welchem Teil der E-Mail gesucht werden soll:
 - Im E-Mail-Betreff. Markieren Sie dazu das Kästchen **Nach Betreff filtern**. Alle E-Mails, deren Betreffzeile mindestens eine Zeichenfolge aus den entsprechenden Tabelle enthält, werden gefiltert.
 - Im Nachrichteninhalte. Markieren Sie dazu das Kästchen **Nach Nachrichteninhalte filtern**. Alle E-Mails, die im Nachrichteninhalte mindestens eine der definierten Zeichenfolgen enthalten, werden gefiltert.
 - Sowohl im Betreff als auch im Inhalt. Markieren Sie dazu beide Kästchen. Alle E-Mails, deren Betreffzeile mit einer Regel aus der ersten Tabelle übereinstimmt UND deren Inhalt mindestens eine Zeichenfolge aus der zweiten Tabelle enthält, werden gefiltert. Zum Beispiel:

Die erste Tabelle enthält die Zeichenfolgen: Newsletter und wöchentlich. Die zweite Tabelle enthält die Zeichenfolgen: Shopping, Preis und Angebot.

Eine E-Mail mit dem Betreff "Monatlicher Newsletter von Ihrem Lieblingsuhrenhersteller" und dem Satz "Wir freuen uns, Ihnen unser neuestes Angebot an spektakulären Uhren zu unwiderstehlichen Preisen zu präsentieren." im Nachrichteninhalte wird gefiltert werden. Wenn der Betreff „Neues von Ihrem Uhrenhersteller“ wäre, würde die E-Mail nicht gefiltert werden.

2. Verwenden Sie die Felder in den Tabellenüberschriften um eine Liste von Bedingungen zu erstellen. Gehen Sie für jede Bedingung wie folgt vor:
 - a. Wählen Sie den Typ der Zeichenfolge, nach der gesucht werden soll. Sie können entweder die genaue Zeichenfolge eingeben oder Textmuster mithilfe von regulären Ausdrücken erstellen.



Beachten Sie

Die Syntax der regulären Ausdrücke muss dem ECMAScript-Standard entsprechen.

- b. Geben Sie die Zeichenfolge in das Feld **Ausdruck** ein.

Zum Beispiel:


- i. Die Zeichenfolge `5[1-5]\d{2}([\s-]?\d{4}){3}` alle Kreditkartennummern bezeichnen, die mit 51 bis 55 beginnen, 16 Stellen in vier Vierergruppen haben, wobei diese Gruppen durch Leerstelle oder Bindestrich getrennt sein können. Daher wird jede E-Mail gefiltert, die z. B. diese Kartennummer in einem der folgenden Formate enthält: 5257-4938-3957-3948, 5257 4938 3957 3948 oder 5257493839573948.
- ii. Über diesen Ausdruck werden E-Mails mit den Worten `Lotter`ie, `Bargeld` und `Preis` in genau dieser Reihenfolge erkannt.

```
(lottery)((.\n|\r)*) ( cash)((.\n|\r)*) ( prize)
```

Um auch E-Mails zu erkennen, die jedes dieser Worte in einer beliebigen Reihenfolge enthalten, fügen Sie drei reguläre Ausdrücke in einer anderen Wortreihenfolge hinzu.

- iii. Über diesen Ausdruck werden E-Mails erkannt, in denen das Wort `Preis` mindestens dreimal vorkommt:

```
(prize)((.\n\r)*) ( prize)((.\n\r)*) ( prize)
```

- c. Wenn Sie möchten, dass Groß- und Kleinschreibung berücksichtigt wird, markieren Sie das Kästchen **Groß./Kleinschr.**. Wenn Sie dieses Kästchen markiert haben, sind zum Beispiel `Newsletter` und `newsletter` nicht mehr dasselbe.
- d. Wenn Sie nicht möchten, dass innerhalb von längeren Wörtern nach der Zeichenfolge gesucht wird, markieren Sie das Kästchen **Ganze Wörter**. Wenn Sie dieses Kästchen markiert haben und z. B. die Zeichenfolge `Gehalt` in der Tabelle ist, wird eine E-Mail, die das Wort `Monatsgehalt` enthält, nicht gefiltert.
- e. Klicken Sie in der Spaltenüberschrift **Aktion** auf die Schaltfläche  **Hinzufügen**, um die Bedingung der Liste hinzuzufügen.
- **Aktionen**. Für E-Mails können Sie verschiedene Aktionen durchführen. Jede dieser Aktionen hat wiederum verschiedene Optionen und/oder sekundäre Aktionen. Sie werden im Folgenden beschrieben:

Hauptaktionen:

- **E-Mail zustellen**. Die erkannte E-Mail wird den Postfächern der Empfänger zugestellt.
- **In die Quarantäne verschieben**. Die E-Mail wird verschlüsselt und im Quarantäne-Ordner des Exchange-Servers gespeichert; sie wird nicht den Empfängern zugestellt. In die Quarantäne verschobene E-Mails können Sie auf der Seite **Quarantäne** verwalten.
- **Umleiten an**. Die E-Mail wird nicht den ursprünglichen Empfängern zugestellt, sondern einem Postfach, das Sie im entsprechenden Feld angeben können.
- **E-Mail ablehnen/löschen**. Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Sekundäre Aktionen:

- **E-Mail-Betreff markieren als**. Sie können dem E-Mail-Betreff eine Bezeichnung hinzufügen, damit andere Benutzer die E-Mail in ihrem Mail-Client filtern können.

- **Der E-Mail einen Header hinzufügen.** Sie können dem Header erkannter E-Mails einen Namen und einen Wert hinzufügen, indem Sie die gewünschten Informationen in die entsprechenden Felder eingeben.
- **E-Mail auf der Festplatte speichern.** Eine Kopie der erkannten E-Mail wird als Datei im angegebenen Ordner auf dem Exchange-Server gespeichert. Wenn der Ordner noch nicht existiert, wird er erstellt. Sie müssen den absoluten Pfad des Ordners in das entsprechende Feld eingeben.



Beachten Sie

Diese Option funktioniert nur mit E-Mails im MIME-Format.

- **Im Konto archivieren.** Eine Kopie der erkannten E-Mail wird an die angegebene E-Mail-Adresse gesendet. Mit dieser Aktion wird die E-Mail-Adresse der Blindkopie-Liste (Bcc-Liste) hinzugefügt.
- Standardmäßig wird eine E-Mail, die die Bedingungen einer Regel erfüllt, nicht mit weiteren Regeln abgeglichen. Wenn Sie jedoch weitere Regeln anwenden möchten, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden**.

Ausschlüsse

Wenn Sie E-Mails mit bestimmten Absendern oder Empfängern unabhängig vom Betreff und Inhalt in jedem Fall zustellen möchten, können Sie hierzu Filterausschlüsse definieren.

So erstellen Sie einen Ausschluss:

1. Klicken Sie dazu auf den Link **Ausschlüsse** neben dem Kästchen **Inhaltsfilterung**. Ein Konfigurationsfenster wird geöffnet.
2. Geben Sie die E-Mail-Adressen der vertrauenswürdigen Absender und/oder Empfänger in die entsprechenden Felder ein. Alle E-Mails von vertrauenswürdigen Absendern oder an vertrauenswürdige Empfänger werden nicht gefiltert. Beim Bearbeiten der Liste können Sie zudem Platzhalter verwenden, um ganze E-Mail-Domains oder ein E-Mail-Adressmuster festzulegen:
 - Sternchen (*) ersetzt kein, ein oder mehrere Zeichen.
 - Fragezeichen (?) ersetzt jeden beliebigen Buchstaben.

Wenn Sie zum Beispiel *.gov eingeben, werden alle eingehenden E-Mails akzeptiert, die über eine .gov-Domain versendet wurden.

3. Wenn Sie E-Mails mit mehreren Empfängern nur dann von der Filterung ausschließen möchten, wenn alle Empfänger auf der Liste vertrauenswürdiger Empfänger stehen, markieren Sie das Kästchen **E-Mail nur dann von der Filterung ausschließen, wenn alle Empfänger vertrauenswürdige sind**.
4. Klicken Sie auf **Speichern**.

Anhangsfilterung

Das Modul Anhangsfilterung bietet Ihnen Filterfunktionen für E-Mail-Anhänge. Mit diesem Modul können Anhänge bestimmter Namensmuster und bestimmter Typen gefiltert werden. Mit der Anhangsfilterung können Sie:

- Potenziell gefährliche Anhänge wie **VBS** oder **EXE**-Dateien blockieren; oder direkt die gesamte E-Mail mit einem dieser Anhänge blockieren.
- Anhänge mit anstößigen Namen blockieren; oder direkt die gesamte E-Mail mit einem dieser Anhänge blockieren.

Anhangsfilterung aktivieren

Wenn Sie die Anhangsfilterung verwenden möchten, markieren Sie das Kästchen **Anhangsfilterung**.

Wie Sie Regeln für die Anhangsfilterung erstellen und verwalten erfahren Sie unter [„Filterregeln verwalten“](#) (S. 389).

Regeloptionen

- **Allgemein**. In diesem Bereich muss ein Name für die Regel eingegeben werden. Sonst kann sie nicht gespeichert werden. Markieren Sie das Kästchen **Aktiv**, wenn sie möchten, dass die Regel gilt, sobald die Richtlinie gespeichert wird.
- **Regel-Anwendungsbereich**. Sie können den Anwendungsbereich einer Regel einschränken, sodass sie nur auf bestimmte E-Mails angewendet wird. Dazu können Sie die folgenden kumulativen Optionen verwenden:
 - **Anwenden auf (Richtung)**. Wählen Sie die Richtung des E-Mail-Datenverkehrs, für die die Regel gelten soll.
 - **Absender**. Hier können Sie einstellen, ob die Regel für alle oder nur für bestimmte Absender gelten soll. Um die Anzahl der Absender einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.
 - **Empfänger**. Hier können Sie festlegen, ob die Regel für alle oder nur für bestimmte Empfänger gelten soll. Um die Anzahl der Empfänger

einzugrenzen, können Sie auf die Schaltfläche **Konkret** klicken und anschließend die gewünschten Gruppen aus der Tabelle links auswählen. Die ausgewählten Gruppen werden in der Tabelle rechts angezeigt.

Die Regel wird angewendet, wenn mindestens ein von Ihnen ausgewählter Empfänger dabei ist. Wenn Sie die Regeln nur anwenden möchten, wenn alle Empfänger in der ausgewählten Gruppe sind, wählen Sie **Alle Empfänger abgleichen**.



Beachten Sie

Die Adressen in den Feldern **Cc** und **Bcc** werden auch als Empfänger angesehen.



Wichtig

Regeln, die auf Benutzergruppen basieren, gelten nur für die Rollen Hub-Transport und Postfach.

- **Einstellungen.** Hier können Sie die Dateitypen angeben, die als E-Mail-Anhänge zugelassen oder blockiert werden sollen.

Sie können E-Mail-Anhänge nach Dateityp oder Dateiname filtern.

So filtern sie Anhänge nach Dateityp:

1. Markieren Sie das Kästchen **Erkennung nach Inhaltstyp**.
2. Wählen Sie die Erkennungsoption, die Ihren Bedürfnissen am besten entspricht:
 - **Nur die folgenden Kategorien**, wenn Sie nur wenige Dateitypenkategorien blockieren möchten.
 - **Alle außer den folgenden Kategorien**, wenn Sie nur wenige Dateitypenkategorien zulassen möchten.
3. Wählen Sie die gewünschten Dateitypenkategorien aus der Liste. Details zu den einzelnen Dateitypenkategorien finden Sie unter [„Dateitypen für die Anhangsfilterung“ \(S. 546\)](#).

Wenn Sie nur einzelne Dateitypen angeben möchten, markieren Sie das Kästchen **Benutzerdefinierte Endungen** und geben Sie die gewünschten Endungen in das entsprechende Feld ein.

4. Markieren Sie das Kästchen **Erkennung des echten Dateityps aktivieren**, um die Datei-Header daraufhin zu überprüfen, um welchen Dateityp es sich bei einem bestimmten Anhang tatsächlich handelt. Das bedeutet, dass eine

schlichte Umbenennung der Dateiendung die Anhaltsfilterung nicht umgehen kann.



Beachten Sie

Die Erkennung der echten Dateitypen kann sehr ressourcenintensiv sein.

Wenn Sie Anhänge nach deren Namen filtern möchten, markieren Sie das Kästchen **Erkennung nach Dateinamen** und geben Sie die Dateinamen, die Sie filtern möchten, in das entsprechende Feld ein. Bei der Bearbeitung der Liste können Sie auch die folgenden Platzhalter verwenden:

- Sternchen (*) ersetzt kein, ein oder mehrere Zeichen.
- Fragezeichen (?) ersetzt jeden beliebigen Buchstaben.

Wenn Sie zum Beispiel `Datenbank.*` eingeben, werden alle Dateien, die `Datenbank` im Namen haben, erkannt.



Beachten Sie

Wenn Sie sowohl die Erkennung nach Inhaltstyp als auch nach Dateinamen aktivieren (ohne Erkennung der echten Dateityps), muss die Datei gleichzeitig beide Bedingungen erfüllen, um gefiltert zu werden. Wenn Sie zum Beispiel die Kategorie **Multimedia** ausgewählt haben und den Dateinamen `Test.pdf` eingegeben haben, wird keine E-Mail gefiltert, weil PDF-Dateien keine Multimedia-Dateien sind.

Markieren Sie das Kästchen **Inhalt von Archiven scannen**, um zu verhindern, dass Dateien, die Sie blockieren möchten, in unauffällig anmutenden Archiven versteckt werden und so Ihren Filter umgehen können.

Innerhalb der Archive ist der Scan rekursiv und geht standardmäßig bis zur vierten Tiefenebene des Archivs. Sie können den Scan wie folgt optimieren:

1. Markieren Sie das Kästchen **Maximale Archvertiefe (Ebenen)**.
2. Wählen Sie aus dem entsprechenden Menü einen anderen Wert aus. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.



Beachten Sie

Wenn Sie den Scan von Archiven aktiviert haben, wird die Option **Inhalt von Archiven scannen** deaktiviert; es werden dann alle Archive gescannt.

- **Aktionen.** Sie können verschiedene Aktionen auf erkannte Anhänge bzw. deren E-Mails durchführen. Jede dieser Aktionen hat wiederum verschiedene Optionen und/oder sekundäre Aktionen. Sie werden im Folgenden beschrieben:

Hauptaktionen:

- **Datei ersetzen.** Entfernt erkannte Dateien und ersetzt sie durch eine Textdatei, die den Benutzer über die durchgeführten Aktionen informiert.

So konfigurieren Sie den Benachrichtigungstext:

1. Klicken Sie dazu auf den Link **Einstellungen** neben dem Kästchen **Anhangsfilterung**.
2. Geben Sie den Benachrichtigungstext in das entsprechende Feld ein.
3. Klicken Sie auf **Speichern**.

- **Datei löschen.** Entfernt die erkannten Dateien ohne Warnung. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **E-Mail ablehnen/löschen.** Auf Servern mit Edge-Transport-Rolle werden die erkannten E-Mails mit SMTP-Fehlercode 550 abgelehnt. In allen anderen Fällen wird die E-Mail ohne Warnung gelöscht. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.
- **E-Mail in die Quarantäne verschieben.** Die E-Mail wird verschlüsselt und im Quarantäne-Ordner des Exchange-Servers gespeichert; sie wird nicht den Empfängern zugestellt. In die Quarantäne verschobene E-Mails können Sie auf der Seite **Quarantäne** verwalten.
- **E-Mail umleiten an.** Die E-Mail wird nicht den ursprünglichen Empfängern zugestellt, sondern an eine E-Mail-Adresse, die Sie im entsprechenden Feld angeben können.
- **E-Mail zu stellen.** Lässt die E-Mail passieren.

Sekundäre Aktionen:

- **E-Mail-Betreff markieren als.** Sie können dem E-Mail-Betreff eine Bezeichnung hinzufügen, damit andere Benutzer die E-Mail in ihrem Mail-Client filtern können.
- **E-Mail-Header hinzufügen.** Sie können dem Header erkannter E-Mails einen Namen und einen Wert hinzufügen, indem Sie die gewünschten Informationen in die entsprechenden Felder eingeben.
- **E-Mail auf der Festplatte speichern.** Eine Kopie der erkannten E-Mail wird als Datei im angegebenen Ordner auf dem Exchange-Server gespeichert. Wenn der Ordner noch nicht existiert, wird er erstellt. Sie

müssen den absoluten Pfad des Ordners in das entsprechende Feld eingeben.



Beachten Sie

Diese Option funktioniert nur mit E-Mails im MIME-Format.

- **Im Konto archivieren.** Eine Kopie der erkannten E-Mail wird an die angegebene E-Mail-Adresse gesendet. Mit dieser Aktion wird die E-Mail-Adresse der Blindkopie-Liste (Bcc-Liste) hinzugefügt.
- Standardmäßig wird eine E-Mail, wenn sie in den Anwendungsbereich einer Regel fällt, ausschließlich gemäß dieser Regel verarbeitet und nicht mit weiteren Regeln abgeglichen. Wenn jedoch die weiteren Regeln auch abgeglichen werden sollen, entfernen Sie die Markierung des Kästchens **Wenn Regel-Bedingungen erfüllt sind, keine weiteren Regeln anwenden**.

Ausschlüsse

Wenn Sie E-Mails mit bestimmten Absendern oder Empfängern unabhängig etwaigen Anhängen in jedem Fall zustellen möchten, können Sie hierzu Filterausschlüsse definieren.

So erstellen Sie einen Ausschluss:

1. Klicken Sie dazu auf den Link **Ausschlüsse** neben dem Kästchen **Anhangsfilterung**. Ein Konfigurationsfenster wird geöffnet.
2. Geben Sie die E-Mail-Adressen der vertrauenswürdigen Absender und/oder Empfänger in die entsprechenden Felder ein. Alle E-Mails von vertrauenswürdigen Absendern oder an vertrauenswürdige Empfänger werden nicht gefiltert. Beim Bearbeiten der Liste können Sie zudem Platzhalter verwenden, um ganze E-Mail-Domains oder ein E-Mail-Adressmuster festzulegen:
 - Sternchen (*) ersetzt kein, ein oder mehrere Zeichen.
 - Fragezeichen (?) ersetzt jeden beliebigen Buchstaben.

Wenn Sie zum Beispiel *.gov eingeben, werden alle eingehenden E-Mails akzeptiert, die über eine .gov-Domain versendet wurden.

3. Wenn Sie E-Mails mit mehreren Empfängern nur dann von der Filterung ausschließen möchten, wenn alle Empfänger auf der Liste vertrauenswürdiger Empfänger stehen, markieren Sie das Kästchen **E-Mail nur dann von der Filterung ausschließen, wenn alle Empfänger vertrauenswürdiger sind**.
4. Klicken Sie auf **Speichern**.

7.2.12. Verschlüsseln



Beachten Sie

Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server
- macOS

Das Verschlüsselungsmodul verwaltet die vollständige Festplattenverschlüsselung auf den Endpunkten, indem es BitLocker unter Windows und FileVault bzw. das Befehlszeilenprogramm diskutil unter macOS nutzt.

Durch diesen Ansatz bietet GravityZone einige attraktive Vorteile:

- Datensicherung bei Verlust oder Diebstahl von Geräten.
- Umfassender Schutz für die weltweit gängigsten Computerplattformen durch Verwendung empfohlener Verschlüsselungsstandards mit voller Unterstützung durch Microsoft und Apple.
- Minimale Auswirkungen auf die Leistung der Endpunkte durch die Nutzung nativer Verschlüsselungstools.

Das Verschlüsselungsmodul setzt die folgenden Lösungen ein:

- BitLocker Version 1.2 und höher, auf Windows-Endpunkten mit Trusted Platform Module (TPM), für bootfähige und nicht bootfähige Laufwerke.
- BitLocker Version 1.2 und höher, auf Windows-Endpunkten ohne TPM, für bootfähige und nicht bootfähige Laufwerke.
- FileVault auf MacOS-Endpunkten, für bootfähige Laufwerke.
- diskutil auf macOS-Endpunkten, für nicht bootfähige Laufwerke.

Die Liste der vom Verschlüsselungsmodul unterstützten Betriebssysteme finden Sie in der GravityZone-Installationsanleitung.

The screenshot shows the 'Verschlüsselung' (Encryption) settings page. On the left is a navigation menu with options like 'Allgemein', 'Malware-Schutz', 'Firewall', 'Netzwerkschutz', 'Anwendungssteuerung', 'Gerätesteuerung', 'Relais', and 'Verschlüsselung'. The 'Verschlüsselung' section is expanded to show 'Allgemein'.

The main content area is titled 'Verschlüsselungsverwaltung' and contains the following options:

- Verschlüsselungsverwaltung**: Wenn Sie dieses Modul aktivieren, können Sie die Endpunktverschlüsselung über das Control Center verwalten. Wenn Sie es deaktivieren, bleiben die Laufwerke im derzeitigen Zustand, in dem die Benutzer die Verschlüsselung dann lokal steuern können.
- Entschlüsseln**: Wählen Sie diese Option, wenn Sie Laufwerke entschlüsseln möchten.
- Verschlüsseln**: Wählen Sie diese Option, wenn Sie Laufwerke verschlüsseln möchten. Benutzer müssen dann ein Passwort eingeben, um sich vor dem Start zu authentifizieren.
 - Wenn das Trusted Platform Module (TPM) aktiv ist, nicht nach dem Pre-Boot-Passwort fragen.
- Ausschlüsse**

Below the options is a table for exclusions:

Typ	Ausgeschlossene Objekte	Aktion
	Entität	+

At the bottom, there is a pagination bar showing 'Erste Seite', 'Seite 0 von 0', 'Letzte Seite', and '20' objects.

Die Verschlüsselungsseite

Um mit der Verwaltung der Endpunktverschlüsselung über das Control Center zu beginnen, markieren Sie das Kontrollkästchen **Verschlüsselungsverwaltung**. Solange diese Einstellung aktiviert ist, können die Endpunktbenutzer die Verschlüsselung nicht lokal verwalten, und alle ihre Aktionen werden abgebrochen oder rückgängig gemacht. Wenn Sie diese Einstellung deaktivieren, bleiben die Endpunktlaufwerke in ihrem aktuellen Zustand (verschlüsselt oder unverschlüsselt), und die Benutzer können die Verschlüsselung auf ihren Computern selbst verwalten.

Zur Verwaltung der Verschlüsselungs- und Entschlüsselungsprozesse stehen Ihnen drei Optionen zur Auswahl:

- **Entschlüsseln** – entschlüsselt Laufwerke und lässt sie entschlüsselt, wenn die Richtlinie auf den Endpunkten aktiv ist.
- **Verschlüsseln** – verschlüsselt Laufwerke und lässt sie verschlüsselt, wenn die Richtlinie auf den Endpunkten aktiv ist.

Unter der Option Verschlüsseln können Sie das Kontrollkästchen **Wenn das Trusted Platform Module (TPM) aktiv ist, nicht nach dem Pre-Boot-Passwort fragen** markieren. Diese Einstellung ermöglicht die Verschlüsselung auf Windows-Endpunkten mit TPM, ohne dass vom Benutzer ein

Verschlüsselungspasswort eingegeben werden muss. Weitere Details dazu finden Sie hier: „[Laufwerke verschlüsseln](#)“ (S. 403).

• Ausschlüsse

GravityZone unterstützt das Advanced Encryption Standard (AES)-Verfahren mit 128- und 256-Bit Schlüsseln unter Windows und macOS. Der tatsächlich verwendete Verschlüsselungsalgorithmus hängt von der jeweiligen Konfiguration des Betriebssystems ab.



Beachten Sie

GravityZone erkennt und verwaltet Laufwerke, die mit BitLocker, FileVault und diskutil manuell verschlüsselt wurden. Um mit der Verwaltung dieser Laufwerke zu beginnen, fordert der Sicherheitsagent die Endpunktbenutzer auf, ihre Wiederherstellungsschlüssel zu ändern. Bei Verwendung anderer Verschlüsselungslösungen müssen die Laufwerke zunächst entschlüsselt werden, bevor eine GravityZone-Richtlinie angewendet wird.

Laufwerke verschlüsseln

So verschlüsseln Sie ein Laufwerk:

1. Markieren Sie das Kontrollkästchen **Verschlüsselungsverwaltung**.
2. Wählen Sie die Option **Verschlüsseln**.

Der Verschlüsselungsvorgang startet, sobald die Richtlinie auf den Endpunkten aktiv wird, wobei unter Windows bzw. Mac jeweils einige Besonderheiten gelten.

Unter Windows

Standardmäßig fordert der Sicherheitsagent den Benutzer auf, ein Passwort zu konfigurieren, um die Verschlüsselung zu starten. Wenn die Maschine über ein funktionsfähiges TPM verfügt, fordert der Sicherheitsagent den Benutzer auf, eine persönliche Identifikationsnummer (PIN) zu konfigurieren, um die Verschlüsselung zu starten. Der Benutzer muss das hier konfigurierte Passwort oder die PIN bei jedem Start des Endpunkts in einem Authentifizierungsbildschirm eingeben, der noch vor dem Systemstart angezeigt wird.



Beachten Sie

Über den Sicherheitsagenten können Sie die Anforderungen an die PIN-Komplexität sowie die Benutzerberechtigungen zum Ändern ihrer PIN in den Einstellungen der BitLocker Group Policy (GPO) konfigurieren.

Wenn Sie die Verschlüsselung starten möchten, ohne dass der Endpunktbenutzer ein Passwort eingeben muss, markieren Sie das Kästchen **Wenn das Trusted Platform Module (TPM) aktiv ist, nicht nach Pre-Boot-Passwort fragen**. Diese Einstellung ist kompatibel mit Windows-Endpunkten mit TPM und UEFI.

Beachten Sie Folgendes, wenn das Kontrollkästchen **Wenn das Trusted Platform Module (TPM) aktiv ist, nicht nach Pre-Boot-Passwort fragen** aktiviert wurde:

- Auf unverschlüsselten Endpunkten:
 - Die Verschlüsselung läuft ohne Passwort.
 - Der Pre-Boot-Authentifizierungsbildschirm wird beim Start der Maschine nicht angezeigt.
- Auf mit Passwort verschlüsselten Endpunkten:
 - Das Passwort wird entfernt.
 - Die Laufwerke bleiben verschlüsselt.
- Auf verschlüsselten oder unverschlüsselten Endpunkten ohne TPM oder mit nicht erkanntem oder nicht funktionsfähigem TPM:
 - Der Benutzer wird aufgefordert, ein Passwort für die Verschlüsselung einzugeben.
 - Der Pre-Boot-Authentifizierungsbildschirm wird beim Start der Maschine angezeigt.

Beachten Sie Folgendes, wenn das Kontrollkästchen **Wenn das Trusted Platform Module (TPM) aktiv ist, nicht nach Pre-Boot-Passwort fragen** deaktiviert wurde:

- Der Benutzer muss ein Passwort für die Verschlüsselung eingeben.
- Die Laufwerke bleiben verschlüsselt.

Unter macOS

Um die Verschlüsselung auf bootfähigen Laufwerken zu starten, fordert der Sicherheitsagent den Benutzer auf, seine Systemanmeldeinformationen einzugeben. Nur Benutzer mit lokalen Konten mit Administratorrechten können die Verschlüsselung aktivieren.

Um die Verschlüsselung auf nicht bootfähigen Laufwerken zu starten, fordert der Sicherheitsagent den Benutzer auf, ein Verschlüsselungspasswort festzulegen. Dieses Passwort wird benötigt, um das nicht bootfähige Laufwerk bei jedem Start des Computers freizuschalten. Wenn der Computer mehr als ein nicht bootfähiges Laufwerk hat, müssen die Benutzer für jedes Laufwerk ein Verschlüsselungspasswort festlegen.

Laufwerke entschlüsseln

So entschlüsseln Sie Laufwerke auf Endpunkten:

1. Markieren Sie das Kontrollkästchen **Verschlüsselungsverwaltung**.
2. Wählen Sie die Option **Entschlüsseln**.

Der Entschlüsselungsvorgang startet, sobald die Richtlinie auf den Endpunkten aktiv wird, wobei unter Windows bzw. Mac jeweils einige Besonderheiten gelten.

Unter Windows

Die Laufwerke werden ohne Eingreifen des Benutzers verschlüsselt.

Unter macOS

Bei bootfähigen Laufwerken muss der Benutzer seine Systemanmeldeinformationen eingeben. Bei nicht bootfähigen Laufwerken muss der Benutzer das während des Verschlüsselungsvorgangs festgelegte Passwort eingeben.


Für den Fall, dass Benutzer ihr Verschlüsselungspasswort vergessen, benötigen sie Wiederherstellungsschlüssel, um ihre Computer zu entsperren. Weitere Details zum Abrufen von Wiederherstellungsschlüsseln finden Sie hier: „[“ \(S. 107\)](#).

Partitionen ausschließen

Wenn Sie bestimmte Laufwerke oder Partitionen von der Verschlüsselung ausschließen möchten, können Sie dies tun, indem Sie einzelne Laufwerksbuchstaben, Partitionsbezeichnungen, -namen oder GUIDs in die Ausschlussliste aufnehmen. Gehen Sie dazu wie folgt vor:

1. Markieren Sie das Kästchen **Ausschlüsse**.
2. Klicken Sie auf **Typ** und wählen Sie einen Laufwerkstyp aus dem Klappmenü.
3. Geben Sie in das Feld **Ausgeschlossene Objekte** einen Wert ein. Dabei haben Sie die folgenden Möglichkeiten:
 - Sie können einen **Laufwerksbuchstaben** gefolgt von einem Doppelpunkt eingeben, z. B. `D:`.
 - Als **Bezeichnung/Name** können Sie z. B. `Arbeit` oder irgendeine andere Bezeichnung eingeben.
 - **A l s G U I D g e b e n S i e z . B .**
`\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\` ein.

4. Klicken Sie auf **Hinzufügen**  um den Ausschluss zur Liste hinzuzufügen.

Wenn Sie einen Ausschluss löschen möchten, markieren Sie einfach den entsprechenden Eintrag und klicken Sie auf **Löschen** .

7.2.13. NSX

In diesem Bereich können Sie festlegen, welche Richtlinie als Sicherheitsprofil in NSX verwendet werden soll. Hierzu müssen Sie:

1. Markieren Sie das Kästchen **NSX**, damit sie auch im vSphere Web Client sichtbar wird.
2. Geben Sie einen Namen ein, unter dem Sie die Richtlinie in NSX wiederfinden können. Dieser Name kann vom Richtliniennamen im GravityZone Control Center abweichen. In vSphere wird Sie mit dem Präfix `Bitdefender_` angezeigt. Wählen Sie den Namen mit Bedacht, da er nach dem Speichern der Richtlinie schreibgeschützt ist.

7.2.14. Speicherschutz

Beachten Sie

Der Speicherschutz ist für Network-Attached Storage (NAS)-Geräte und File-Sharing-Lösungen verfügbar, die mit dem Internet Content Adaptation Protocol (ICAP) kompatibel sind.

In diesem Bereich können Sie Security Server als Scan-Dienst für NAS-Geräte und ICAP-kompatible File-Sharing-Lösungen wie Nutanix Files und Citrix ShareFile konfigurieren.

Security Server scannen auf Anfrage durch die Speichergeräte beliebige Dateitypen, auch Archive. Abhängig von den Einstellungen ergreifen Security Server geeignete Maßnahmen für infizierte Dateien, so z. B. Desinfizieren oder Zugriffsverweigerung.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [ICAP](#)
- [Ausschlüsse](#)

ICAP

Sie können die folgenden Optionen für Security Server konfigurieren:

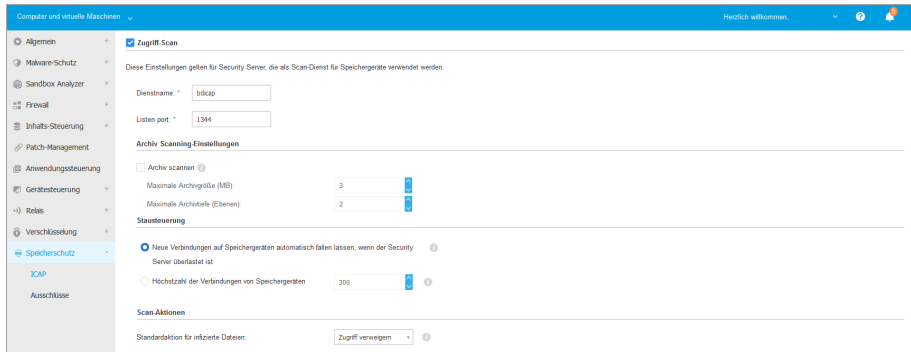
- Markieren Sie das Kästchen **Zugriff-Scan**, um das Modul für den Speicherschutz zu aktivieren. Die für die Kommunikation zwischen Security Servern und den Speichergeräten erforderlichen Einstellungen sind wie folgt vordefiniert:
 - Dienstname: `bdicap`.
 - Listen-Port: 1344.
- Markieren Sie unter **Archiv Scanning-Einstellungen** das Kästchen **Archiv scannen**, um Archiv-Scans zu aktivieren. Legen Sie die maximale Größe und die maximale Tiefe der zu scannenden Archive fest.



Beachten Sie

Wenn Sie die maximale Größe des Archivs auf 0 (Null) setzen, scannt Security Server Archive unabhängig von ihrer Größe.

- Wählen Sie unter **Stausteuerung** die bevorzugte Methode zur Verwaltung der Verbindungen auf Speichergeräten, falls es zu einer Überlastung des Security Servers kommt:
 - **Neue Verbindungen auf Speichergeräten automatisch trennen, wenn der Security Server überlastet ist.** Wenn ein Security Server die maximale Anzahl an Verbindungen erreicht hat, leitet das Speichergerät den Überschuss auf einen zweiten Security Server um.
 - **Höchstzahl der Verbindungen von Speichergeräten.** Der Standardwert ist auf 300 Verbindungen eingestellt.
- Unter **Scan-Aktionen** stehen die folgenden Optionen zur Auswahl:
 - **Zugriff verweigern** – Security Server verweigert den Zugriff auf infizierte Dateien.
 - **Desinfizieren** – Security Server entfernt den Schadcode aus den infizierten Dateien.



Richtlinien- Speicherschutz - ICAP

Ausschlüsse

Wenn Sie bestimmte Objekte vom Scan ausschließen möchten, markieren Sie das Kästchen **Ausschlüsse**.


Sie können Ausschlüsse definieren:

- Per Hash - Sie identifizieren die ausgeschlossene Datei per Hash SHA-256.
- Per Platzhalter – Sie identifizieren die ausgeschlossene Datei nach Pfad.

Ausschlüsse konfigurieren

Um einen Ausschluss hinzuzufügen:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. Je nach Ausschlussart geben Sie das auszuschließende Objekt wie folgt an:
 - **Hash** – geben Sie SHA-256-Hashwerte durch Komma getrennt ein.
 - **Platzhalter** – geben Sie einen absoluten oder relativen Pfadnamen an, indem Sie Platzhalterzeichen verwenden. Das Sternchen (*) steht für jede Datei innerhalb eines Verzeichnisses. Ein Fragezeichen (?) steht für genau ein beliebiges Zeichen.
3. Fügen Sie eine Beschreibung für den Ausschluss hinzu.
4. Klicken Sie auf den Button **+Hinzufügen**. Der neue Ausschluss wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu löschen, klicken Sie auf den entsprechenden **Löschen**-Link .

Importieren und Exportieren von Ausschlüssen

Wenn Sie Ausschlüsse in weiteren Richtlinien wiederverwenden möchten, können Sie sie exportieren und wieder importieren.

So können Sie Ausschlüsse exportieren:

1. Klicken Sie dazu oben an der Ausschlusstabelle auf **Exportieren**.
2. Speichern Sie die CSV-Datei auf Ihrem Computer. Je nach den Browser-Einstellungen wird die Datei automatisch heruntergeladen oder Sie werden aufgefordert, einen Speicherort für sie zu wählen.

Jede Zeile in der CSV-Datei entspricht einem Ausschluss. Die Reihenfolge der Felder ist wie folgt:

```
<exclusion type>, <object to be excluded>, <description>
```

Dies sind die möglichen Werte für die CSV-Felder:

Ausschlussart:

- 1, für Hash SHA-256
- 2, für Platzhalter

Auszuschließendes Objekt:

Ein Hashwert oder Pfadname

Beschreibung

Text zum einfacheren Auffinden des Ausschlusses.

Beispiel für Ausschlüsse in der CSV-Datei:

```
2,*/file.txt,text  
2,*/image.jpg,image  
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

So können Sie Ausschlüsse importieren:

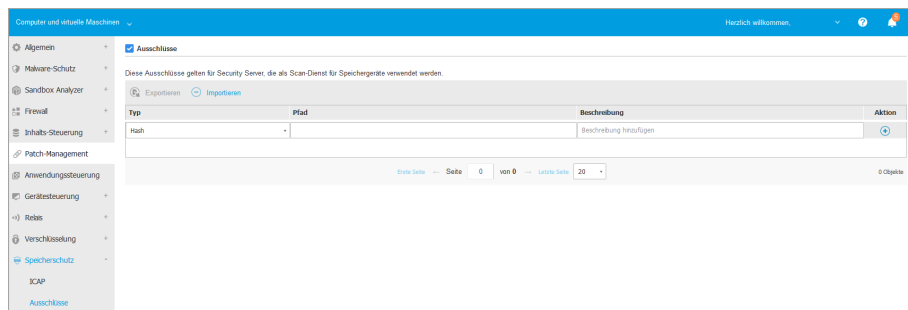
1. Klicken Sie auf **Importieren**. Das Fenster **Richtlinienausschlüsse importieren** wird geöffnet.

2. Klicken Sie auf **Hinzufügen** und wählen Sie dann die CSV-Datei.
3. Klicken Sie auf **Speichern**. Die Tabelle wird mit den gültigen Ausschlüssen ausgefüllt. Wenn eine CSV-Datei ungültige Ausschlüsse enthält, werden Sie durch eine Meldung auf die entsprechenden Zeilennummern hingewiesen.

Ausschlüsse bearbeiten

So können Sie einen Ausschluss bearbeiten:

1. Klicken Sie in der Spalte **Pfad** oder in der Beschreibung auf den Namen des Ausschlusses.
2. Bearbeiten Sie den Ausschluss.
3. Drücken Sie nach Abschluss die **Eingabetaste**.



Richtlinien- Speicherschutz - ICAP

7.3. Richtlinien für Mobilgeräte

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.

So konfigurieren Sie die Einstellungen einer Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie **Mobilgeräte** aus der **Ansichtsauswahl**.
3. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinieneinstellungsseite
4. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Es gibt die folgenden Kategorien von Einstellungen:

- **Allgemein**
 - Details
- **Geräteverwaltung**
 - Sicherheit
 - Passwort
 - Profile

Sie können die Einstellungskategorie über das Menü auf der linken Seite auswählen.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und auf die gewünschten Mobilgeräte anzuwenden. Wenn Sie die Richtlinienseite verlassen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

7.3.1. Allgemein

Die Kategorie **Allgemein** enthält nähere Informationen zur ausgewählten Richtlinie.

Details

Auf der Seite Details finden Sie allgemeine Informationen zur jeweiligen Richtlinie:

- Richtliniename
- Benutzer, der die Richtlinie angelegt hat
- Datum und Zeitpunkt, zu dem die Richtlinie erstellt wurde.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde

Sie können die Richtlinie umbenennen, indem Sie einen neuen Namen in das entsprechende Feld eingeben. Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.



Beachten Sie

Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

7.3.2. Geräteverwaltung

Über die Einstellungen der Geräteverwaltung können Sie Sicherheitsoptionen für Mobilgeräte definieren, eine Bildschirmsperre mit Passwort einrichten und mehrere Profile für jede Mobilgeräte-Richtlinie anlegen.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- [Sicherheit](#)
- [Passwort](#)
- [Profile](#)

Sicherheit

In diesem Bereich können Sie verschiedene Sicherheitseinstellungen für Mobilgeräte konfigurieren, darunter Malware-Scans für Android-Geräte, Verwaltung von inoffiziell entsperrten Geräten oder die Aktion, die bei nicht-konformen Geräten ausgeführt werden soll.



Wichtig

Die Malware-Scans werden in der Cloud durchgeführt, weshalb die Mobilgeräte Internet-Zugang benötigen.

<ul style="list-style-type: none"> ⚙ Allgemein + 📁 Geräteverwaltung - <li style="padding-left: 20px;">Sicherheit <li style="padding-left: 20px;">Passwort <li style="padding-left: 20px;">Profile 	<h4>Android-Sicherheit</h4> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Anwendungen bei der Installation scannen <input checked="" type="checkbox"/> Speicher beim Einhängen scannen <input type="checkbox"/> Geräteverschlüsselung erfordern ⓘ <input checked="" type="checkbox"/> USB-Debugging-Schutz <input checked="" type="checkbox"/> Web-Sicherheit <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Phishing-Webseiten blockieren <input checked="" type="checkbox"/> Webseiten, die Malware oder Exploits enthalten, blockieren <input checked="" type="checkbox"/> Webseiten, die Teil eines Betrugs sind, blockieren <input checked="" type="checkbox"/> Benutzer vor nicht-vertrauenswürdigen Webseiten warnen <hr/> <h4>Änderungen im Betriebssystem</h4> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Verwaltung inoffiziell entsperrter Geräte (Jailbreak oder Rooting) zulassen ⓘ <hr/> <h4>Konformität</h4> <p>Standardaktion, wenn ein geschäftliches Gerät nicht konform ist: Ignorieren ▾</p> <p>Standardaktion, wenn ein privates Gerät nicht konform ist: Ignorieren ▾</p>
--	---

Mobilgeräterichtlinien - Sicherheitseinstellungen

Android-Sicherheit

- Wählen Sie **Anwendungen bei der Installation scannen**, wenn Sie möchten, dass neue Anwendungen gescannt werden, wenn sie auf verwalteten Mobilgeräten installiert werden.
- Wählen Sie **Speicher beim Einhängen scannen**, wenn Sie Speichergeräte gescannt werden sollen, wenn sie eingehängt werden.

Warnung

Wenn Malware gefunden wird, wird der Benutzer aufgefordert, sie zu entfernen. Wenn der Benutzer gefundene Malware nicht innerhalb von einer Stunde nach dem Fund entfernt, wird das Mobilgerät für nicht-konform erklärt, und die eingestellte Nichtkonformitätsaktion wird automatisch ausgeführt (ignorieren, Zugriff verweigern, sperren, löschen oder Verknüpfung aufheben).

- Wählen Sie **Geräteverschlüsselung erfordern**, um den Benutzer aufzufordern, die Verschlüsselungsfunktion von Android zu aktivieren. Durch die Verschlüsselung wird verhindert, dass Unbefugte auf Daten wie Konten, Einstellungen, heruntergeladene Anwendungen, Medien und andere Dateien, die auf dem Android-Gerät gespeichert sind, zugreifen. Von außen kann nur mithilfe des entsprechenden Passworts auf die verschlüsselten Daten zugegriffen werden.

Wichtig

- Geräteverschlüsselung steht für Betriebssysteme ab Android 3.0 zur Verfügung. Nicht alle Gerätemodelle unterstützen die Verschlüsselung. Unter **Mobilgerätedetails** sehen Sie, ob die Verschlüsselung unterstützt wird.
- Die Verschlüsselung kann sich auf die Leistung des Geräts auswirken.

Warnung

- Die Geräteverschlüsselung kann nicht rückgängig gemacht werden: Der nicht verschlüsselte Zustand kann nur durch eine vollständige Löschung des Geräts wiederhergestellt werden.
- Legen Sie Sicherheitskopien Ihrer Daten an, bevor Sie die Geräteverschlüsselung aktivieren.
- Der Verschlüsselungsvorgang darf nicht unterbrochen werden; es besteht sonst die Gefahr von Datenverlust.

Wenn Sie diese Option aktivieren, zeigt GravityZone Mobile Client dauerhaft eine Meldung an, die den Benutzer auffordert, die Verschlüsselung zu aktivieren. Der Benutzer muss dann auf die Schaltfläche **Beheben** tippen, um den Verschlüsselungsbildschirm anzuzeigen und den Verschlüsselungsvorgang zu starten. Wenn die Verschlüsselung nicht innerhalb von 7 Tagen nach der Aufforderung aktiviert wird, ist das Gerät nicht mehr konform.

So aktivieren Sie die Verschlüsselung auf einem Android-Gerät:

- Der Akku muss noch zu mindestens 80 % voll sein.
- Das Gerät muss angeschlossen bleiben, bis die Verschlüsselung abgeschlossen ist.
- Der Benutzer muss ein Passwort zur Entsperrung einrichten, das die Sicherheitsanforderungen erfüllt.



Beachten Sie

- Android-Geräte verwenden dasselbe Passwort zur Entsperrung des Bildschirms und zur Entsperrung verschlüsselter Daten.
- Zur Verschlüsselung wird ein Passwort, eine PIN oder das richtige Gesicht benötigt, und alle anderen Bildschirmensperreinstellungen werden deaktiviert.

Der Verschlüsselungsvorgang kann 1 Stunde oder länger dauern. Währenddessen wird das Gerät eventuell mehrmals neu gestartet.

Im Fenster **Mobilgerätdetails** können Sie den Speicherverschlüsselungsstatus jedes Mobilgeräts sehen.

- Android-Geräte im USB-Debugging-Modus können über ein USB-Kabel mit einem PC verbunden werden, wodurch der Zugriff auf das Betriebssystem und die Apps erweitert wird. Dies bedeutet eine Gefahr für die Sicherheit dieser Mobilgeräte. Die Funktion **USB-Debugging-Schutz**, die standardmäßig aktiviert ist, verhindert, dass Geräte im USB-Debugging-Modus verwendet werden können. Wenn der Benutzer das USB-Debugging aktiviert, wird das Gerät automatisch nicht-konform und die entsprechende Nichtkonformitätsaktion wird ausgeführt. Wenn die Nichtkonformitätsaktion **Ignorieren** ist, wird der Benutzer auf die unsichere Einstellung hingewiesen.

Dennoch können Sie diese Option für Mobilgeräte, die im USB-Debugging-Modus laufen müssen (z. B. Mobilgeräte, die zum Entwickeln und Testen von Apps genutzt werden) deaktivieren.

- Wählen Sie **Web-Sicherheit**, um Web-Sicherheitsfunktionen auf Android-Geräten zu aktivieren.

Die Web-Sicherheit scannt jede URL, auf die zugegriffen wird, in der Cloud und sendet dann einen Sicherheitsstatus an GravityZone Mobile Client. Es gibt die folgenden URL-Sicherheitsstatus: sauber, Betrug, Malware, Phishing oder nicht vertrauenswürdig.

GravityZone Mobile Client kann je nach URL-Sicherheitsstatus eine bestimmte Aktion ausführen:

- **Phishing-Webseiten blockieren.** Wenn der Benutzer versucht, auf eine Phishing-Website zuzugreifen, blockiert GravityZone Mobile Client die entsprechende URL und zeigt stattdessen einen Warnhinweis an.
- **Webseiten, die Malware oder Exploits enthalten, blockieren.** Wenn der Benutzer versucht, auf eine Website zuzugreifen, die Malware oder Web-Exploits verbreitet, blockiert GravityZone Mobile Client die entsprechende URL und zeigt stattdessen einen Warnhinweis an.
- **Webseiten, die Teil eines Betrugs sind, blockieren.** Dehnt den Schutz auf andere Arten von Betrügereien außer Phishing aus (zum Beispiel auf gefälschte Escrows, gefälschte Spendenaufrufe, Missbrauch sozialer Netzwerke usw.). Wenn der Benutzer versucht, auf eine betrügerische Website zuzugreifen, blockiert GravityZone Mobile Client die entsprechende URL und zeigt stattdessen einen Warnhinweis an.
- **Benutzer vor nicht-vertrauenswürdigen Webseiten warnen.** Wenn der Benutzer auf eine Website zugreift, die zuvor zu Phishing-Zwecken gehackt wurde oder kürzlich über Spam- oder Phishing-E-Mails verbreitet wurde, wird eine Pop-up-Warnung angezeigt, die Webseite aber nicht blockiert.



Wichtig

Die Web-Sicherheitsfunktionen werden nur bis Android 5 sowie nur in Chrome und dem integrierten Android-Browser unterstützt.

Änderungen im Betriebssystem

Da sie für Unternehmensnetzwerke als Sicherheitsrisiko gelten, werden inoffiziell entsperrte Geräte (durch sog. Jailbreak oder Rooting) automatisch für nicht-konform erklärt.

- Wählen Sie **Verwaltung inoffiziell entsperrter Geräte (Jailbreak oder Rooting) zulassen**, wenn Sie inoffiziell entsperrte Geräte vom Control Center aus verwalten möchten. Da solche Geräte standardmäßig nicht konform sind, wird auf sie automatisch die eingestellte **Nichtkonformitätsaktion** angewendet, sobald sie erkannt werden. Wenn Sie also auf solchen Geräten Richtlinien anwenden oder Aufgaben ausführen möchten, müssen Sie als Nichtkonformitätsaktion Ignorieren wählen.
- Wenn Sie den Haken aus dem Kästchen **Verwaltung inoffiziell entsperrter Geräte (Jailbreak oder Rooting) zulassen** entfernen, heben Sie automatisch die Verknüpfung zwischen inoffiziell entsperrten Geräten und dem GravityZone-Netzwerk auf. In diesem Fall zeigt die Anwendung GravityZone Mobile Client eine Nachricht an, dass das Gerät inoffiziell entsperrt wurde (Rooting bzw. Jailbreak). Der Benutzer kann auf die OK-Schaltfläche tippen, um zum Registrierungsbildschirm zu gelangen. Sobald die inoffizielle Entsperrung des Geräts rückgängig gemacht wurde oder die Richtlinie dahingehend verändert wurde, dass inoffizielle entsperrte Geräte verwaltet werden können, kann das Gerät neu registriert werden (mit demselben Token bei Android-Geräten bzw. mit einem neuen Token bei iOS-Geräten).

Konformität

Sie können je nach Eigentümer eines Geräts (Unternehmen oder privat) bestimmte Aktionen konfigurieren, die automatisch ausgeführt werden sollen, wenn ein Gerät als nicht konform erkannt wird.

Beachten Sie

Wenn Sie im Control Center ein neues Gerät hinzufügen, werden Sie aufgefordert, den Eigentümer des Geräts (Unternehmen oder privat) anzugeben. So kann GravityZone private und Unternehmensgeräte getrennt voneinander verwalten.

- **Kriterien für Nichtkonformität**
- **Nichtkonformitätsaktionen**

Kriterien für Nichtkonformität

Ein Gerät wird in den folgenden Fällen für nicht konform erklärt:

● Android-Geräte

- Gerät wurde inoffiziell entsperrt (Rooting).
- GravityZone Mobile Client ist nicht Geräteadministrator.
- Malware wird nicht innerhalb von einer Stunde nach dem Fund entfernt.
- Richtlinie nicht erfüllt:
 - Der Benutzer legt nicht innerhalb von 24 Stunden nach der ersten Benachrichtigung ein Passwort für die Bildschirmentsperrung fest.
 - Der Benutzer ändert dass Passwort für die Bildschirmentsperrung nicht zur vorgegebenen Zeit.
 - Der Benutzer aktiviert die Geräteverschlüsselung nicht innerhalb von sieben Tagen nach der ersten Aufforderung.
 - Der USB-Debugging-Modus ist auf dem Gerät aktiviert, solange die USB-Debugging-Schutz-Richtlinie aktiviert ist.

● iOS-Geräte

- Gerät wurde inoffiziell entsperrt (Jailbreak).
- GravityZone Mobile Client wurde auf dem Gerät deinstalliert.
- Richtlinie nicht erfüllt:
 - Der Benutzer legt nicht innerhalb von 24 Stunden nach der ersten Benachrichtigung ein Passwort für die Bildschirmentsperrung fest.
 - Der Benutzer ändert dass Passwort für die Bildschirmentsperrung nicht zur vorgegebenen Zeit.

Standardaktion, wenn das Gerät nicht konform ist

Wenn ein Gerät für nicht-konform erklärt wird, wird der Benutzer aufgefordert, das Konformitätsproblem zu beheben. Der Benutzer muss die nötigen Änderungen innerhalb einer vorgegebenen Zeit durchführen; sonst wird die eingestellte Aktion für nicht-konforme Geräte ausgeführt (ignorieren, Zugriff verweigern, sperren, löschen oder Verknüpfung aufheben).

Sie können die Nichtkonformitätsaktion jederzeit in der Richtlinie ändern. Die neue Aktion wird auf nicht-konforme Geräte angewendet, sobald die Richtlinie gespeichert wird.

Wählen Sie aus dem Menü jeder Geräteeigentümerart die Aktion, die ausgeführt werden soll, wenn ein Gerät als nicht konform eingestuft wird:

- **Ignorieren.** Meldet dem Benutzer nur, dass das Gerät nicht konform zur Nutzungsrichtlinie für Mobilgeräte ist.
- **Zugriff verweigern.** Blockiert den Zugriff des Geräts auf Unternehmensnetzwerke, indem die WLAN- und VPN-Einstellungen gelöscht, aber alle anderen in der Richtlinie definierten Einstellungen beibehalten werden. Blockierte Einstellungen werden wiederhergestellt, sobald das Gerät wieder konform ist.



Wichtig

Wenn für GravityZone Mobile Client Geräteadministrator deaktiviert ist, wird das Gerät nicht-konform, und die Aktion **Zugriff verweigern** wird automatisch angewendet.

- **Sperrern.** Sperrt sofort den Bildschirm des Geräts.
 - Unter Android wird der Bildschirm nur dann mit einem durch GravityZone generiertes Passwort gesperrt, wenn auf dem Gerät selbst kein Sperrschutz konfiguriert wurde. Eine bereits konfigurierte Sperroption wie Muster, PIN, Passwort, Fingerabdruck oder Smart Lock wird dadurch nicht überschrieben.
 - Auf iOS-Geräten mit einem bestehenden Passwort zur Entsperrung des Bildschirms wird dieses zum Entsperren abgefragt.
- **Löschen.** Stellt den Auslieferungszustand des Geräts wieder her, wobei alle Benutzerdaten unwiederbringlich gelöscht werden.



Beachten Sie

Diese Option löscht derzeit keine Daten von eingehängten Geräten (SD-Karten).

- **Verknüpfung aufheben.** Das Gerät wird sofort vom Netzwerk entfernt.



Beachten Sie

Um ein aus dem Netzwerk entferntes Mobilgerät wieder im Netzwerk zu registrieren, müssen Sie das Gerät erneut im Control Center hinzufügen. Dann muss das Gerät mit einem neuen Aktivierungs-Token erneut registriert werden.

Bevor Sie das tun, sollten Sie aber die Umstände, die zur Aufhebung der Verknüpfung mit dem Netzwerk geführt haben, beseitigen oder die Richtlinieneinstellungen so verändern, dass das Gerät wieder verwaltet werden kann.

Passwort

In diesem Bereich können Sie die Funktion der Bildschirmspernung per Passwort aktivieren, die im Betriebssystem des Mobilgeräts vorhanden ist.

⚙️ Allgemein	<input checked="" type="checkbox"/> Bildschirmsperre mit Passwort Einstellungen
📱 Geräteverwaltung	
Sicherheit	<input type="radio"/> - Aggressiv Normal - durchschnittliche Passwortsicherheit
Passwort	Benötigt 12-Zeichen-Passwörter (mindestens 2 komplexe Zeichen). Bildschirm wird nach 3 Minuten gesperrt. Passwörter gelten für 3 Monate, und die jeweils letzten 4 Passwörter können nicht erneut verwendet werden.
Profile	<input type="radio"/> - Tolerant
	<input type="radio"/> Benutzerdef.

Mobilgeräterichtlinien - Passwortschutzeinstellungen

Wenn diese Funktion einmal aktiviert ist, wird der Benutzer aufgefordert, ein Passwort zur Bildschirmspernung festzulegen. Der Benutzer muss ein Passwort festlegen, das die in der Richtlinie festgelegten Passwortanforderungen erfüllt. Wenn der Benutzer das Passwort festgelegt hat, werden alle Benachrichtigungen diesbezüglich gelöscht. Im Folgenden kann der Bildschirm dann nur noch mit diesem Passwort entsperrt werden.

Beachten Sie

Wenn der Benutzer kein Passwort festlegt, nachdem er dazu aufgefordert wurde, kann der Bildschirm des Geräts bis zu 24 Stunden nach der ersten Benachrichtigung ohne Passwort entsperrt werden. Während dieser Zeit wird der Benutzer alle 15 Minuten über eine Nachricht auf dem Bildschirm dazu aufgefordert, ein Passwort zur Bildschirmspernung festzulegen.

Warnung

Wenn der Benutzer nicht innerhalb von 24 Stunden nach der ersten Benachrichtigung ein Passwort festlegt, wird das Gerät nicht-konform, und die [die eingestellte Aktion für nicht-konforme Geräte](#) wird ausgeführt.

So konfigurieren Sie die Einstellungen für Passwörter zur Bildschirmspernung:

1. Markieren Sie das Kästchen **Bildschirmsperre mit Passwort**.

2. Klicken Sie auf die Passwort-Sicherheitsstufe, die Ihren Anforderungen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.
3. Wenn Sie detailliertere Einstellungen vornehmen möchten, wählen Sie die Stufe **Benutzerdefiniert** und klicken dann auf den Link **Einstellungen**.

Passwort-Einstellungen ✕

Konfiguration

Typ:

Alphanumerischer Wert erforderlich

Mindestlänge

Mindestanzahl an komplexen Zeichen

Ablauffrist (Monate)

Wiederholungsbeschränkung (vergangene
Passwörter)

Höchstzahl an Fehlversuchen

Automatische Sperre nach (Minuten)

Mobilgeräterichtlinien - erweiterte Passwortschutzeinstellungen



Beachten Sie

Sie können die Passwortkonfigurationsanforderungen einer voreingestellten Sicherheitsstufe einsehen, indem Sie auf den Link **Einstellungen** klicken. Wenn Sie irgendeine Option ändern, wechselt die Sicherheitsstufe automatisch zu **Benutzerdefiniert**.

Benutzerdefinierte Optionen.

- **Typ.** Sie können festlegen, ob ein einfaches Passwort reicht oder ob es ein komplexes sein muss. Passwortkomplexitätskriterien sind im Betriebssystem des Mobilgeräts definiert.

- Auf Android-Geräten muss ein komplexes Passwort mindestens einen Buchstaben, eine Ziffer und ein Sonderzeichen enthalten.



Beachten Sie

Komplexe Passwörter werden ab Android 3.0 unterstützt.

- Auf iOS-Geräten werden in komplexen Passwörtern keine sequenziellen oder wiederholten Zeichen (also abcdef, 12345 oder aaaaa, 11111) zugelassen. Je nach gewählter Option überprüft das Betriebssystem, ob das vom Benutzer festgelegte Passwort die Kriterien erfüllt und meldet dem Benutzer, falls es sie nicht erfüllt.
- **Alphanumerischer Wert erforderlich.** Das Passwort muss sowohl Buchstaben als auch Ziffern beinhalten.
- **Mindestlänge.** Das Passwort muss mindestens eine bestimmte Länge haben, die Sie im entsprechenden Feld festlegen können.
- **Mindestanzahl an komplexen Zeichen.** Das Passwort muss mindestens eine bestimmte Zahl an nicht-alphanumerischen Zeichen beinhalten (also z. B. @, # oder \$), die Sie im entsprechenden Feld festlegen können.
- **Ablauffrist (Monate).** Der Benutzer muss das Passwort zur Bildschirmspernung in einem regelmäßigen Abstand ändern (in Monaten). Wenn Sie also z. B. 3 eingeben, wird der Benutzer alle 3 Monate aufgefordert, das Passwort zu ändern.



Beachten Sie

Auf Android-Geräten wird diese Funktion ab der Version 3.0 unterstützt.

- **Wiederholungsbeschränkung (vergangene Passwörter).** Wählen Sie eine Zahl oder geben Sie sie in das entsprechende Feld ein, die festlegt, wie viele der jeweils letzten Passwörter nicht wiederverwendet werden dürfen. Wenn Sie z. B. 4 eingeben, kann der Benutzer keines seiner 4 letzten Passwörter als neues Passwort benutzen.



Beachten Sie

Auf Android-Geräten wird diese Funktion ab der Version 3.0 unterstützt.

- **Höchstzahl an Fehlversuchen.** Hier können Sie festlegen, wie oft der Benutzer ein falsches Passwort eingeben kann.

**Beachten Sie**

Wenn Sie eine höhere Zahl als 6 festlegen, wird bei iOS-Geräten nach dem sechsten falsch eingegebenen Passwort eine Zeitsperre aktiviert, bevor der Benutzer erneut versuchen kann, das Passwort einzugeben. Die Zeitsperre wird mit jedem Fehlversuch länger.

**Warnung**

Wenn der Benutzer die Höchstzahl an Fehlversuchen zur Bildschirmspernung überschreitet, werden alle Daten und Einstellungen auf dem Gerät gelöscht.

- **Automatische Sperre nach (Minuten).** Hier können Sie festlegen, nach wie vielen Minuten Inaktivität das Gerät automatisch gesperrt wird.

**Beachten Sie**

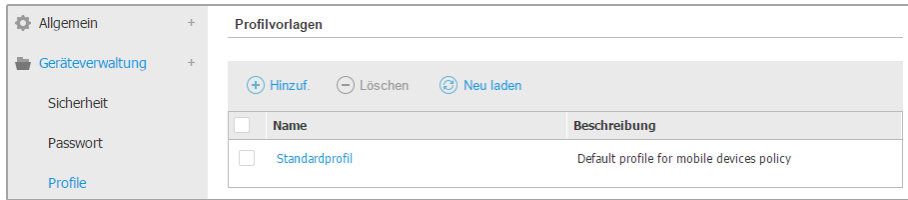
iOS-Geräte haben eine festgelegte Liste von Zeiten für die automatische Sperre und lassen keine benutzerdefinierten Werte zu. Wenn eine Richtlinie mit einem inkompatiblen Wert für die Automatische Sperre zugewiesen wurde, wendet das Gerät den nächsten restriktiveren Zeitraum aus der Liste an. Wenn in der Richtlinie z. B. ein Zeitraum von 3 Minuten für die Automatische Sperre eingestellt ist, wird das Gerät automatisch nach 2 Minuten Inaktivität gesperrt.

Wenn Sie die Richtlinie verändern und damit eine höhere Sicherheitsstufe für das Passwort zur Bildschirmspernung wählen, werden die Benutzer aufgefordert, das Passwort den neuen Kriterien anzupassen.

Wenn Sie die Option **Bildschirmsperre mit Passwort** deaktivieren, erhalten die Benutzer wieder die volle Kontrolle über die Bildschirmspernfunktion ihres Mobilgeräts. Das bestehende Passwort bleibt aktiv, bis der Benutzer es ändert oder löscht.

Profile

In diesem Bereich können Sie Nutzungsprofile für Mobilgeräte erstellen, verändern und löschen. Mit Nutzungsprofilen können Sie WLAN- und VPN-Einstellungen per Push übertragen und die Internet-Zugangssteuerung auf verwalteten Mobilgeräten anwenden.



Mobilgeräterichtlinien - Profilvorlagen

Sie können mehrere Profile anlegen, es kann aber immer nur jeweils ein Profil pro Gerät aktiv sein.

- Wenn Sie nur ein Profil anlegen, wird dieses automatisch auf allen Geräten angewendet, denen die Richtlinie zugewiesen ist.
- Wenn Sie mehrere Profile anlegen, wird das erste Profil in der Liste automatisch auf allen Geräten angewendet, denen die Richtlinie zugewiesen ist.

Benutzer von Mobilgeräten können das zugewiesene Profil und die Einstellungen jedes Profils in der Anwendung GravityZone Mobile Client einsehen. Benutzer können die bestehenden Einstellungen eines Profils nicht ändern, aber sie können ein anderes wählen, wenn mehrere verfügbar sind.



Beachten Sie

Zum Wechseln des Profils muss eine Internetverbindung bestehen.

So erstellen Sie ein neues Profil:

1. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle. Die Profilkonfigurationsseite wird angezeigt.
2. Konfigurieren Sie die Einstellungen nach Bedarf. Detaillierte Informationen finden Sie unter:
 - „Details“ (S. 424)
 - „Netzwerke“ (S. 424)
 - „Internet-Zugang“ (S. 428)
3. Klicken Sie auf **Speichern**. Das neue Profil wird der Liste hinzugefügt.

Sie können ein oder mehrere Profile löschen, indem Sie das bzw. die entsprechende(n) Kästchen markieren und dann auf die Schaltfläche **- Löschen** auf der rechten Seite der Tabelle klicken.

Um ein Profil zu ändern, klicken Sie auf seinen Namen, ändern Sie die gewünschten Einstellungen, und klicken Sie anschließend auf **Speichern**.

Details

Die Seite **Details** enthält allgemeine Informationen zu dem Profil:

- **Name.** Geben Sie den gewünschten Profilnamen ein. Profile sollten aussagekräftige Namen tragen, damit Sie oder andere Administratoren diese schnell identifizieren können.
- **Beschreibung.** Geben Sie hier eine Beschreibung des Profils ein. Dadurch können Administratoren besser erkennen, um welches Profil es sich handelt.

Netzwerke

In diesem Bereich können Sie die Einstellung eines oder mehrerer WLAN- und VPN-Netzwerke festlegen. Die VPN-Einstellungen stehen nur für iOS-Geräte zur Verfügung.

The screenshot shows the 'Profile' configuration page in the GravityZone console. On the left is a navigation menu with 'Profile', 'Details', 'Netzwerke', and 'Internetzugang'. The main content area is titled 'WLAN' and contains a table for adding and managing wireless networks. Above the table are buttons for '+ Hinzuf.', '- Löschen', 'Neu laden', 'hoch', and 'runter'. The table has columns for 'Priorität', 'Name', and 'Verschlüsselung'. Below this is a section for 'VPN für iOS' with a similar table and control buttons.

Mobilgeräterichtlinien - Netzwerkverbindungseinstellungen des Profils





Wichtig

Bevor sie WLAN- und VPN-Verbindungen definieren, sollten Sie sicherstellen, dass Sie alle nötigen Informationen zur Hand haben (Passwörter, Proxy-Einstellungen usw.).


Die Mobilgeräte, denen das entsprechende Profil zugewiesen ist, stellen automatisch eine Verbindung zum festgelegten Netzwerk her, sofern es in Reichweite ist. Wenn Sie mehrere Netzwerke erstellen, können Sie Prioritäten festlegen, denn es kann immer nur ein Netzwerk gleichzeitig genutzt werden. Wenn das erste Netzwerk nicht verfügbar ist, versucht das Mobilgerät eine Verbindung zum zweiten herzustellen, usw.

So legen Sie Prioritäten für die Netzwerke fest:

1. Markieren Sie das Kästchen des gewünschten Netzwerks.
2. Klicken Sie auf die Prioritätsschaltflächen auf der rechten Seite der Tabelle:
 - Mit der Schaltfläche  **Hoch** erhöhen Sie die Priorität des ausgewählten Netzwerks.
 - Mit der Schaltfläche  **Runter** verringern Sie die Priorität.

● WLAN

Sie können so viele WLAN-Netzwerke hinzufügen, wie Sie möchten. So fügen Sie ein WLAN-Netzwerk hinzu:

1. Klicken Sie im Bereich **WLAN** auf die Schaltfläche  **Hinzufügen** auf der rechten Seite der Tabelle. Ein Konfigurationsfenster wird geöffnet.
2. Im Reiter **Allgemein** können Sie die Details des WLAN-Verbindung konfigurieren:
 - **Name (SSID)**. Geben Sie den Namen des neuen WLAN-Netzwerks ein.
 - **Sicherheit**. Wählen Sie passende Sicherheitsstufe für das WLAN-Netzwerk:
 - **Keine**. Wählen Sie diese Option, wenn die WLAN-Verbindung öffentlich ist (keine Zugangsdaten erforderlich).
 - **WEP**. Wählen Sie diese Option für eine WEP-verschlüsselte Verbindung. Geben Sie das für diese Art der Verbindung nötige Passwort in das entsprechende Feld ein.
 - **WPA/WPA2 privat**. Wählen Sie diese Option für ein WPA-verschlüsseltes Netzwerk. Geben Sie das für diese Art der Verbindung nötige Passwort in das entsprechende Feld ein.

3. Unter **TCP/IP** können Sie die TCP/IP-Einstellungen für die WLAN-Verbindung konfigurieren. Jede WLAN-Verbindung kann IPv4 oder IPv6 oder beide verwenden.
 - **IPv4 konfigurieren.** Wenn Sie IPv4 verwenden möchten, wählen Sie die IP-Zuweisungsmethode aus dem entsprechenden Menü:
 - DHCP:** wenn die IP-Adresse automatisch von einem DHCP-Server zugewiesen wird. Geben Sie, wenn nötig, die DHCP-Client-ID in das folgende Feld ein.
 - Deaktiviert:** Wählen Sie diese Option, wenn Sie das IPv4-Protokoll nicht verwenden möchten.
 - **IPv6 konfigurieren.** Wenn Sie IPv6 verwenden möchten, wählen Sie diese IP-Zuweisungsmethode aus dem entsprechenden Menü:
 - DHCP:** wenn die IP-Adresse automatisch von einem DHCP-Server zugewiesen wird.
 - Deaktiviert:** Wählen Sie diese Option, wenn Sie das IPv6-Protokoll nicht verwenden möchten.
 - **DNS-Server.** Geben Sie die Adresse mindestens eines DNS-Servers für das Netzwerk ein.
4. Unter dem Reiter **Proxy** können Sie die Proxy-Einstellungen für die WLAN-Verbindung konfigurieren. Wählen Sie die gewünschte Proxy-Konfigurationsmethode aus dem Menü **Typ**:
 - **Aus.** Wählen Sie diese Option, wenn das WLAN-Netzwerk keine Proxy-Einstellungen hat.
 - **Manuell.** Wählen Sie diese Option, um die Proxy-Einstellungen manuell festzulegen. Geben Sie den Hostnamen des Proxy-Servers ein sowie den Port, auf dem es auf Verbindungen lauscht. Wenn der Proxy-Server eine Authentifizierung erfordert, markieren Sie das Kästchen **Authentifizierung**, und geben Sie Benutzernamen und Passwort in die folgenden Felder ein.
 - **Automatisch.** Wählen Sie diese Option, um die Proxy-Einstellungen von einer im Netzwerk veröffentlichten PAC-Datei (proxy auto configuration) zu beziehen. Geben Sie die Adresse der PAC-Datei in das Feld **URL** ein.
5. Klicken Sie auf **Speichern**. Die neue WLAN-Verbindung wird der Liste hinzugefügt.

- **VPN für iOS**

Sie können so viele VPNs hinzufügen, wie nötig. So fügen Sie ein VPN hinzu:

1. Klicken Sie im Bereich **VPN für iOS** auf die Schaltfläche  **Hinzufügen** auf der rechten Seite der Tabelle. Ein Konfigurationsfenster wird geöffnet.
2. Legen Sie im Fenster **VPN-Verbindung** die VPN-Einstellungen fest:

Allgemein:

- **Name.** Geben Sie den Namen der VPN-Verbindung ein.
- **Verschlüsselung.** Für diesen Verbindungstyp steht das Authentifizierungsprotokoll **IPSec** zur Verfügung, für das Benutzerauthentifizierung per Passwort und Maschinenauthentifizierung per gemeinsamem Geheimnis erforderlich sind.
- **Server.** Geben Sie die Adresse des VPN-Servers ein.
- **Benutzer.** Geben Sie den VPN-Benutzernamen ein.
- **Passwort.** Geben Sie das VPN-Passwort ein.
- **Gruppenname.** Geben Sie den Gruppennamen ein.
- **Geheimnis.** Geben Sie den vorher vereinbarten Schlüssel (PSK) ein.


Proxy:

In diesem Bereich können Sie die Proxy-Einstellungen für die VPN-Verbindung konfigurieren. Wählen Sie die gewünschte Proxy-Konfigurationsmethode aus dem Menü **Typ**:

- **Aus.** Wählen Sie diese Option, wenn die VPN-Verbindung keine Proxy-Einstellungen hat.
- **Manuell.** Mit dieser Option können Sie die Proxy-Einstellungen manuell festlegen.
 - **Server:** Geben Sie hier den Proxy-Hostnamen ein.
 - **Port:** Geben Sie hier die Proxy-Portnummer ein.
 - Wenn der Proxy-Server eine Authentifizierung erfordert, markieren Sie das Kästchen **Authentifizierung**, und geben Sie Benutzernamen und Passwort in die folgenden Felder ein.

- **Automatisch.** Wählen Sie diese Option, um die Proxy-Einstellungen von einer im Netzwerk veröffentlichten PAC-Datei (proxy auto configuration) zu beziehen. Geben Sie die Adresse der PAC-Datei in das Feld **URL** ein.

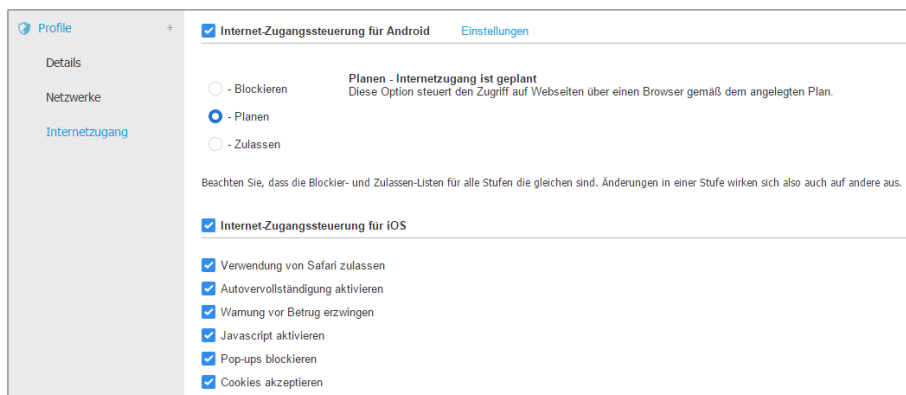
3. Klicken Sie auf **Speichern**. Die neue VPN-Verbindung wird der Liste hinzugefügt.

Sie können ein oder mehrere Netzwerke löschen, indem Sie das bzw. die entsprechende(n) Kästchen markieren und dann auf die Schaltfläche  **Löschen** auf der rechten Seite der Tabelle klicken.

Um ein Netzwerk zu ändern, klicken Sie auf seinen Namen, ändern Sie die gewünschten Einstellungen, und klicken Sie anschließend auf **Speichern**.

Internet-Zugang

In diesem Bereich können Sie die Internet-Zugangsteuerung für Android- und iOS-Geräte konfigurieren.



The screenshot shows the 'Internetzugang' settings page. On the left, a sidebar contains 'Profile', 'Details', 'Netzwerke', and 'Internetzugang'. The main content area is titled 'Internet-Zugangsteuerung für Android' with an 'Einstellungen' link. It features three radio button options: 'Blockieren', 'Planen', and 'Zulassen'. The 'Planen' option is selected, and a message states 'Planen - Internetzugang ist geplant' with a sub-note: 'Diese Option steuert den Zugriff auf Webseiten über einen Browser gemäß dem angelegten Plan.' Below this, a warning reads: 'Beachten Sie, dass die Blockier- und Zulassen-Listen für alle Stufen die gleichen sind. Änderungen in einer Stufe wirken sich also auch auf andere aus.' The 'Internet-Zugangsteuerung für iOS' section is checked and includes several sub-options: 'Verwendung von Safari zulassen', 'Autovervollständigung aktivieren', 'Warnung vor Betrug erzwingen', 'Javascript aktivieren', 'Pop-ups blockieren', and 'Cookies akzeptieren'.

Mobilgeräterichtlinien - Internet-Zugriffseinstellungen des Profils

- **Internet-Zugangsteuerung für Android.** Aktivieren Sie diese Option, um den Internetzugriff für Chrome und den eingebauten Android-Browser zu filtern. Sie können eine zeitliche Begrenzung des Internetzugriffs festlegen und bestimmte Webseite explizit zulassen oder blockieren. Die Webseiten die von der Internet-Zugangsteuerung blockiert werden, werden nicht im Browser angezeigt. Stattdessen wird eine Standardseite angezeigt, die den Nutzer darüber informiert,

dass die angeforderte Webseite von der Internet-Zugangssteuerung blockiert wurde.



Wichtig

Die Internet-Zugangssteuerung für Android wird nur bis Android 5 sowie nur in Chrome und dem integrierten Android-Browser unterstützt.

Sie haben drei Konfigurationsoptionen:

- Mit **Zulassen** lassen Sie den Internetzugriff immer zu.
- Mit **Blockieren** lassen Sie den Internetzugriff nie zu.
- Mit **Planen** können Sie einen Zeitplan für den Internetzugriff festlegen.

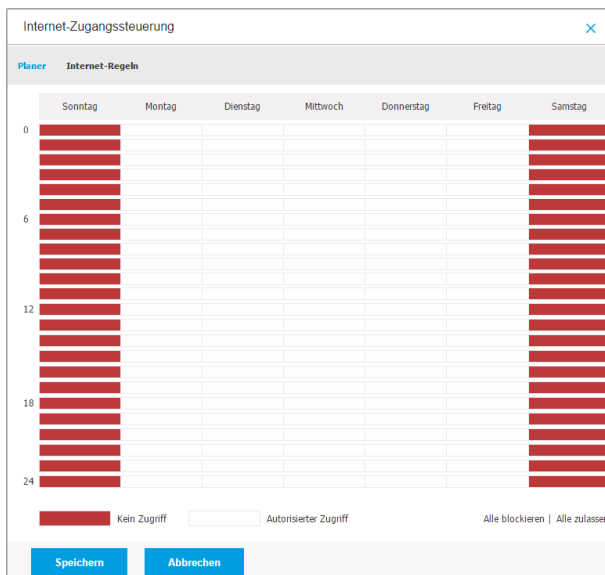
Wenn Sie den Internetzugriff zulassen oder blockieren, können Sie Ausnahmen zu diesen Einstellungen definieren; für ganze Internetkategorien oder für bestimmte einzelne Internetadressen. Klicken Sie auf **Einstellungen** und konfigurieren Sie den Zeitplan bzw. die Ausnahmen wie folgt:

Planer

So schränken Sie den Internet-Zugang auf bestimmte Tageszeiten während der Woche ein:

1. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert werden soll.

Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.



Mobilgerätorichtlinien - Internet-Zugriffsplanung

Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.

2. Klicken Sie auf **Speichern**.

Internet-Regeln

Sie können auch Internetregeln erstellen, um bestimmte Internet-Adressen konkret zu blockieren oder zuzulassen. Diese Regeln ignorieren die Einstellungen der Internet-Zugangssteuerung. Wenn also zum Beispiel der Internetzugang durch die Internet-Zugangssteuerung blockiert ist, können Benutzer trotzdem auf bestimmte Webseiten zugreifen.

So legen Sie eine Internetregel an:

1. Wählen Sie **Ausnahmen verwenden**, um Internet-Ausnahmen zu verwenden.
2. Geben Sie die Adresse, die Sie zulassen oder blockieren möchten in das Feld **Internetadresse** ein.
3. Wählen Sie **Zulassen** oder **Blockieren** aus dem Menü **Berechtigung**.

4. Klicken Sie auf die Schaltfläche **+** **Hinzufügen** auf der rechten Seite der Tabelle, um die Adresse der Liste der Ausnahmen hinzuzufügen.

5. Klicken Sie auf **Speichern**.

So bearbeiten Sie eine Internet-Regel:

1. Klicken Sie auf die Internet-Adresse, die Sie bearbeiten wollen:

2. Die bestehende URL verändern.

3. Klicken Sie auf **Speichern**.

So entfernen Sie eine Internet-Regel:

1. Bewegen Sie den Mauszeiger über die Internetadresse, die Sie entfernen möchten.

2. Klicken Sie auf die Schaltfläche **×** **Löschen**.

3. Klicken Sie auf **Speichern**.

Mit Platzhaltern können Sie Web-Adressenmuster definieren:

- Ein Sternchen (*) ersetzt null oder mehr Zeichen.
- Ein Fragezeichen (?) ersetzt genau ein Zeichen. Sie können mehrere Fragezeichen benutzen, um eine beliebige Kombination einer bestimmten Anzahl von Zeichen zu ersetzen. So steht ??? z. B. für eine beliebige Folge von genau drei Zeichen.

In der folgenden Tabelle finden Sie eine Reihe von Beispielsyntaxen für die Angabe von Internet-Adressen.

Syntax	Anwendungsbereich
www.beispiel*	Jeder Website oder Web-Seite, die mit <code>www.beispiel</code> beginnt (unabhängig von der Domänenenerweiterung). Die Regel gilt nicht für die Unterdomänen der angegebenen Website, so zum Beispiel <code>unterdomäne.beispiel.com</code> .
*beispiel.com	Jede Website, die mit <code>beispiel.com</code> aufhört, einschließlich aller Seiten und Unterdomänen.

Syntax	Anwendungsbereich
Zeichenfolge	Jeder Website oder Web-Seite, in deren Adresse die angegebene Zeichenfolge enthalten ist.
*.com	Jede Website mit der Domänenerweiterung .com, einschließlich aller Seiten und Unterdomänen. Mit dieser Syntax können Sie eine gesamte Top-Level-Domain vom Scan ausschließen.
www.beispiel?.com	Jede Internet-Adresse, die mit www.beispiel?.com beginnt. Das Fragezeichen kann dabei für jedes beliebige einzelne Zeichen stehen. Beispiele hierfür sind www.beispiel1.com oder www.beispielA.com.

- **Internet-Zugangssteuerung für iOS.** Aktivieren Sie diese Option, wenn Sie die Einstellungen des eingebauten iOS-Browsers (Safari) zentral verwalten möchten. Benutzer von Mobilgeräten werden diese Einstellungen dann nicht mehr selbst auf ihrem Gerät ändern können.
 - **Verwendung von Safari zulassen.** Mit dieser Option können Sie steuern, ob der Browser Safari auf Mobilgeräten benutzt werden kann. Wenn Sie diese Option deaktivieren, wird die Safari-Verknüpfung von der iOS-Oberfläche entfernt, sodass die Benutzer nicht mehr über Safari auf das Internet zugreifen können.
 - **Autovervollständigung aktivieren.** Deaktivieren Sie diese Option, wenn Sie verhindern möchten, dass der Browser Formulareingaben speichert (da diese vertrauliche Informationen enthalten können).
 - **Warnung vor Betrug erzwingen.** Aktivieren Sie diese Option, wenn Sie sicherstellen möchten, dass Benutzer gewarnt werden, wenn sie auf betrügerische Webseiten zugreifen.
 - **Javascript aktivieren.** Deaktivieren Sie diese Option, wenn Sie möchten, dass Safari Javascript auf Websites ignoriert.
 - **Pop-ups blockieren.** Aktivieren Sie diese Option, wenn Sie verhindern möchten, dass Pop-up-Fenster automatisch geöffnet werden.

- **Cookies akzeptieren.** Safari akzeptiert Cookies standardmäßig. Deaktivieren Sie diese Option, wenn Sie verhindern möchten, dass Websites Informationen über den Browser-Verlauf speichern.



Wichtig

Internet-Zugangssteuerung für iOS wird unter iOS 13 nicht unterstützt.

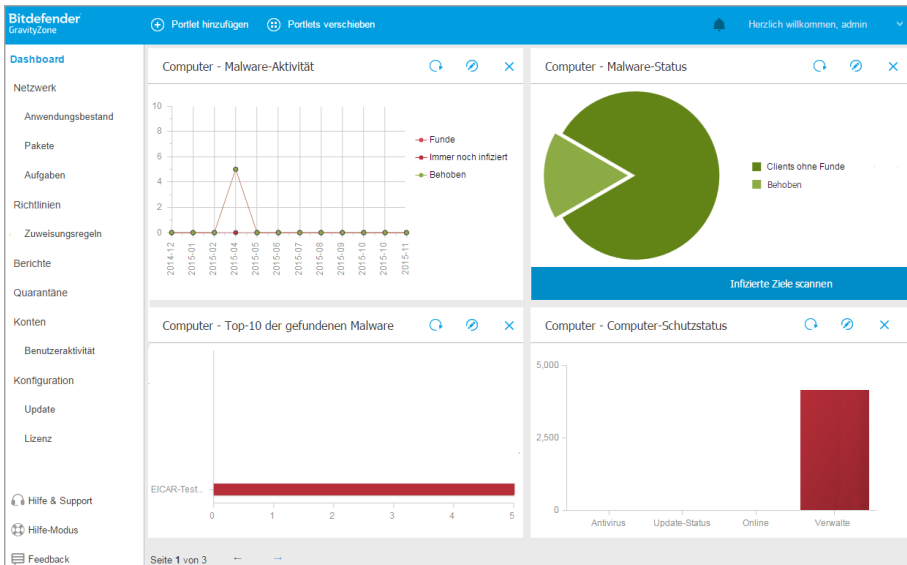
8. ÜBERWACHUNGS-DASHBOARD

Die ordnungsgemäße Analyse Ihrer Netzwerksicherheit erfordert Datenzugriff und -korrelation. Zentral verfügbare Sicherheitsinformationen ermöglichen es Ihnen, die Einhaltung der Sicherheitsrichtlinien des Unternehmens zu überwachen und sicherzustellen, Probleme schnell zu identifizieren und Bedrohungen und Schwachstellen zu analysieren.

8.1. Dashboard

Das Control Center-Dashboard ist eine individuell anpassbare Oberfläche, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Endpunkte und den Netzwerkstatus verschafft.

In den Dashboard-Portlets werden verschiedenste Echtzeit-Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie bieten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.



Das Dashboard

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center verfügt über verschiedene vordefinierte Dashboard-Portlets.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Es gibt eine Reihe verschiedener Portlet-Typen, die unterschiedliche Informationen über den Schutz Ihrer Endpunkte enthalten, so zum Beispiel Update-Status, Malware-Status, Firewall-Aktivität.



Beachten Sie

Standardmäßig rufen die Portlets Daten für den heutigen Tag ab. Im Gegensatz zu Berichten können sie nicht auf Intervalle eingestellt werden, die länger als ein Monat sind.

- Die in den Portlets angezeigten Informationen beziehen sich nur auf Endpunkte unter Ihrem Konto. Sie können die Ziele und Präferenzen jedes Portlets mit dem Befehl **Portlet bearbeiten** an Ihre Bedürfnisse anpassen.
- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Die Portlets werden in Vierergruppen angezeigt. Mit der senkrechten Scroll-Leiste oder den Pfeiltasten können Sie von einer Portlet-Gruppe zur nächsten navigieren.
- Bei verschiedenen Berichtstypen haben Sie die Möglichkeit, sofort bestimmte Aufgaben auf den Zielendpunkten ausführen zu lassen, ohne dazu erst auf die Seite **Netzwerk** wechseln zu müssen; so können Sie z. B. infizierte Endpunkte scannen oder Endpunkte aktualisieren. Über die Schaltfläche am unteren Rand des Portlets können Sie **die entsprechende Aktion ausführen**.


Das Dashboard lässt sich nach individuellen Vorlieben leicht konfigurieren. Sie können Portlet-Einstellungen **bearbeiten**, neue Portlets **hinzufügen**, Portlets **entfernen** oder die bestehenden Portlets **neu anordnen**.

8.1.1. Portlet-Daten neu laden

Um sicherzustellen, dass das Portlet die aktuellsten Informationen anzeigt, klicken Sie auf die Schaltfläche **Neu laden** in der entsprechenden Titelleiste.

Um die Daten in allen Portlets gleichzeitig zu aktualisieren, klicken Sie oben im Dashboard auf die Schaltfläche **Portlets aktualisieren**.


8.1.2. Portlet-Einstellungen bearbeiten

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an. Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die das Symbol  **Portlet bearbeiten** in der entsprechenden Titelleiste klicken.

8.1.3. Ein neues Portlet hinzufügen

Sie können andere Portlets hinzufügen, um bestimmte Informationen angezeigt zu bekommen.


So fügen Sie ein neues Portlet hinzu:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche  **Portlet hinzufügen** am oberen Rand der Konsole. Das Konfigurationsfenster wird geöffnet.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:
 - Endpunkttyp (**Computer**, **Virtuelle Maschinen** oder **Mobile Geräte**)
 - Art des Hintergrundberichts
 - Aussagekräftiger Portlet-Name
 - Das Intervall, in dem die Ereignisse berichtet werden

Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter [„Berichtstypen“](#) (S. 438).

4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die Sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

8.1.4. Ein Portlet entfernen

Sie können ein Portlet ganz einfach entfernen, indem Sie in seiner Titelleiste auf das Symbol  **Entfernen** klicken. Wenn Sie ein Portlet einmal entfernt haben, können Sie es nicht wiederherstellen. Sie können aber ein neues Portlet mit genau denselben Einstellungen erstellen.

8.1.5. Portlets neu anordnen

Sie können die Portlets im Dashboard ganz nach Ihren Bedürfnissen anordnen. So ordnen Sie die Portlets neu an:

1. Gehen Sie zur Seite **Dashboard**.

2. Ziehen Sie die einzelnen Portlets mit der Maus an die gewünschte Stelle. Alle anderen Portlets zwischen der alten und der neuen Position behalten ihre Anordnung bei.

**Beachten Sie**

Sie können Portlets nur innerhalb der bestehenden Positionen verschieben.

9. BERICHTE VERWENDEN

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Netzwerkobjekte zentral erstellen und anzeigen. Die Berichte können zu verschiedenen Zwecken eingesetzt werden, wie zum Beispiel:

- Einhaltung der Unternehmenssicherheitsrichtlinien überwachen und sicherstellen.
- Überprüfung und Bewertung des Netzwerksicherheitsstatus.
- Sicherheitsprobleme, Bedrohungen und Sicherheitslücken im Netzwerk erkennen.
- Sicherheitsvorfälle überwachen
- Bereitstellung von übersichtlichen Daten zur Netzwerksicherheit für die Unternehmensführung.

Es stehen verschiedene Berichtstypen zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten. Diese Informationen werden in übersichtlichen interaktiven Diagrammen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Die Berichte können Daten vom gesamten Netzwerk der verwalteten Netzwerkobjekte beinhalten oder sich auf ausgewählte Gruppen konzentrieren. So können Sie mit einem einzigen Bericht folgendes erfahren:

- Statistische Daten zu allen oder Gruppen von verwalteten Netzwerkobjekten.
- Detailinformationen für jedes verwaltete Netzwerkobjekt.
- Die Liste von Computern, die bestimmte Kriterien erfüllen (zum Beispiel solche, deren Malware-Schutz deaktiviert ist).

Einige Berichte ermöglichen es Ihnen auch, die in Ihrem Netzwerk gefundenen Probleme schnell und unkompliziert zu beheben. So können Sie z. B. direkt aus dem Bericht heraus alle gewünschten Netzwerkobjekte aktualisieren, ohne eine Aktualisierungsaufgabe von der Seite **Netzwerk** ausführen zu müssen.

Alle geplanten Berichte stehen im Control Center zur Verfügung, Sie können sie aber auch auf Ihrem Computer speichern oder per E-Mail versenden.

Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

9.1. Berichtstypen

Für jeden Endpunkttyp stehen eine Reihe von Berichtstypen zur Verfügung:

- [Berichte zu Computern und virtuellen Maschinen](#)
- [Exchange-Berichte](#)
- [Berichte zu Mobilgeräten](#)

9.1.1. Berichte zu Computern und virtuellen Maschinen

Im Folgenden werden die verschiedenen Berichtstypen für physische und virtuelle Maschinen beschrieben:

Phishing-Schutz-Aktivität

Informiert Sie über die Aktivität des Phishing-Schutz-Moduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten Phishing-Websites auf den ausgewählten Endpunkten sowie den Benutzer anzeigen, der zum Zeitpunkt der letzten Erkennung angemeldet war. Sie können auf die Links in der Spalte **Blockierte Websites** klicken, um die URLs der Websites anzuzeigen, wie oft und wann sie zuletzt blockiert wurden.

Blockierte Anwendungen

Informiert Sie über die Aktivitäten der folgenden Module: Malware-Schutz, Firewall, Inhaltssteuerung, Anwendungssteuerung, Erweiterter Exploit-Schutz, ATC/IDS und HVI. Sie können die Anzahl der blockierten Anwendungen auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Klicken Sie auf die einem Ziel zugehörige Zahl, um weitere Informationen zu den blockierten Anwendungen, der Anzahl der Ereignisse und dem Datum und dem Zeitpunkt des zuletzt blockierten Ereignisses anzuzeigen.

In diesem Bericht können Sie die Sicherheitsmodule bequem anweisen, die Ausführung der ausgewählten Anwendung auf dem Zielpunkt zuzulassen:

- Klicken Sie auf die Schaltfläche **Ausnahme hinzufügen**, um Ausnahmen in den folgenden Modulen festzulegen: Malware-Schutz, ATC, Inhaltssteuerung, Firewall und HVI. Es erscheint ein Bestätigungsfenster mit Informationen zu der neuen Regel, welche die bestehende Richtlinie für diesen spezifischen Endpunkt modifiziert.
- Klicken Sie auf die Schaltfläche **Regel hinzufügen**, um eine Regel für eine Anwendung oder einen Prozess in der Anwendungssteuerung festzulegen. Über das Konfigurationsfenster können Sie die Regel auf eine bestehende Richtlinie anwenden. Eine Nachricht informiert Sie über die neue Regel, die die diesem Endpunkt zugewiesene Richtlinie verändert. Der Bericht zeigt

zudem die Anzahl der versuchten Zugriffe und ob das Modul im Testmodus oder im Produktivmodus betrieben wurde.

Blockierte Webseiten

Informiert Sie über die Aktivität des Moduls Internet-Zugangssteuerung von Bitdefender Endpoint Security Tools. Für jedes Ziel können Sie die Anzahl der blockierten Websites sehen. Wenn Sie auf eine dieser Zahlen klicken, können Sie zusätzliche Informationen anzeigen:

- URL und Kategorie der Website
- Anzahl der versuchten Aufrufe pro Website
- Datum und Zeitpunkt des letzten Versuchs sowie den Benutzer, der zum Zeitpunkt der Erkennung angemeldet war.
- Gründe für die Blockierung. Hierzu gehören: geplanter Zugriff, Erkennung von Malware, Kategorienfilterung und Blacklists.

Datenschutz

Informiert Sie über die Aktivität des Identitätsschutzmoduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten E-Mails und Websites auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Aktivität der Gerätesteuerung

Informiert Sie über Ereignisse beim Zugriff auf die Endpunkte über überwachte Geräte. Sie können für jeden Zielpunkt die Anzahl der zugelassenen/blockierten Zugriffs- und Schreibgeschützt-Ereignisse anzeigen. Wenn Ereignisse eingetreten sind, können Sie zusätzliche Informationen dazu anzeigen, indem Sie auf die entsprechenden Zahlen klicken. Angezeigt werden Details zu:

- Auf der Maschine angemeldeter Benutzer
- Gerätetyp und -ID
- Gerätehersteller und Produkt-ID
- Datum und Uhrzeit des Ereignisses.

Status der Endpunktverschlüsselung

Liefert Daten zum Verschlüsselungsstatus der Endpunkte. In einem Kuchendiagramm wird die Anzahl der mit den

Verschlüsselungsrichtlinieneinstellungen konformen bzw. nicht-konformen Maschinen dargestellt.

In einer Tabelle unter dem Kuchendiagramm werden unter anderem folgende Details angezeigt:

- Endpunkt-Name.
- Full Qualified Domain Name (FQDN).
- IP-Adresse der Maschine.
- Betriebssystem.
- Konformität mit der Geräterichtlinie:
 - **Konform** – wenn sämtliche Laufwerke verschlüsselt oder unverschlüsselt sind, je nach Richtlinie.
 - **Nicht-konform** – wenn der Status des Laufwerks nicht mit der zugewiesenen Richtlinie übereinstimmt (z. B. nur eins von zwei Laufwerken verschlüsselt ist oder ein Verschlüsselungsvorgang gerade noch auf dem Laufwerk läuft).
- Geräterichtlinie (**Verschlüsseln** oder **Entschlüsseln**).
- Klicken Sie auf die Zahlen in der Spalte Laufwerkzusammenfassung, um Informationen zu den Laufwerken jedes Endpunkts zu erhalten: ID, Name, Verschlüsselungsstatus (**Verschlüsselt** oder **Unverschlüsselt**), Probleme, Typ (**Boot** oder **Nicht boot-fähig**), Größe, Wiederherstellungsschlüssel-ID.

Status der Endpunktmodule

Ermöglicht einen Überblick über die Abdeckung durch Sicherheitsmodule auf den ausgewählten Zielen. In den Berichtsdetails können Sie für jeden Zielendpunkt anzeigen, welche Module aktiv, deaktiviert oder nicht installiert sind und welche Scan-Engine verwendet wird. Mit einem Klick auf den Namen des Endpunkts öffnen Sie das Fenster **Informationen**, in dem Sie Details zum Endpunkt und den installierten Schutzebenen finden.

Mit einem Klick auf **Client neu konfigurieren** können Sie eine Aufgabe starten, um die Anfangseinstellungen eines oder mehrerer ausgewählter Endpunkte zu ändern. Einzelheiten finden Sie unter [Client neu konfigurieren](#).

Status des Endpunktschutzes

Bietet Ihnen verschiedene Statusinformationen zu ausgewählten Endpunkten in Ihrem Netzwerk.

- Status des Malware-Schutzes
- Update-Status von Bitdefender Endpoint Security Tools
- Status der Netzwerkaktivität (online/offline)
- Verwaltungsstatus

Sie können nach Sicherheitsaspekt und -status filtern, um die Informationen zu erhalten, nach denen Sie suchen.

Firewallaktivität

Informiert Sie über die Aktivität des Firewall-Moduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten Verbindungsversuche und Port-Scans auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

HyperDetect-Aktivität

Informiert Sie über die Aktivität des HyperDetect-Moduls von Bitdefender Endpoint Security Tools.

Im Diagramm im oberen Bereich der Berichtsseite werden die Dynamiken des Angriffsversuchs während des festgelegten Zeitraums sowie die Verteilung der Angriffsarten angezeigt. Wenn Sie mit dem Mauszeiger über die Einträge in der Legende fahren, wird die entsprechende Angriffsart im Diagramm hervorgehoben. Wenn Sie auf einen Eintrag klicken, wird die entsprechende Zeile im Diagramm angezeigt bzw. ausgeblendet. Wenn Sie auf eine beliebige Stelle einer Zeile klicken, werden die Daten in der Tabelle gemäß dem ausgewählten Typ gefiltert. Wenn Sie zum Beispiel an irgendeiner Stelle auf die orangefarbene Zeile klicken, werden in der Tabelle nur Exploits angezeigt.

Über die Details im unteren Bereich des Berichts können Sie die Schwachstellen in Ihrem Netzwerk identifizieren und nachsehen, ob sie behoben wurden. Sie beziehen sich auf:

- Der Pfad zu der Malware-Datei bzw. die gefundene URL im Falle von infizierten Dateien. Bei dateilosen Angriffen wird der Name der für den Angriff verwendeten ausführbaren Datei zusammen mit einem Link zu einem Detailfenster mit Informationen zum Grund der Erkennung und der schädlichen Befehlszeilen-Zeichenfolge angezeigt.
- Der Endpunkt, auf dem der Fund gemacht wurde
- das Sicherheitsmodul, das die Bedrohung gefunden hat. Da HyperDetect eine zusätzliche Schicht der Module Malware-Schutz und Inhaltssteuerung

ist, enthält der Bericht Informationen im Zusammenhang mit einem dieser beiden Module. Welche, hängt von der Art des Fundes ab.

- Der Art des beabsichtigten Angriffs (gezielter Angriff, Grayware, Exploit, Ransomware, verdächtige Dateien und Netzwerkdatenverkehr)
- Der Bedrohungsstatus
- Der Sicherheitsstufe, auf der die Bedrohung entdeckt wurde (tolerant, normal, aggressiv)
- die Anzahl der Male, die die Bedrohung gefunden wurde
- der jüngste Fund
- Erkennung als dateiloser Angriff (ja oder nein), um die Funde von dateilosen Angriffen schnell und einfach filtern zu können



Beachten Sie

Eine Datei kann in verschiedenen Angriffen vorkommen. Daher meldet GravityZone sie für jede Angriffsart, in der sie vorkam.

In diesem Bericht können Sie Fehlalarme einfach ausschließen, indem Sie in den zugewiesenen Sicherheitsrichtlinien Ausnahmen definieren. Hierzu müssen Sie:

1. Wählen Sie so viele Einträge in der Tabelle aus, wie Sie brauchen.



Beachten Sie

Die Erkennung von dateilosen Angriffen kann nicht zur Liste der Ausnahmen hinzugefügt werden, da es sich bei der gefundenen ausführbaren Datei selbst nicht um Malware handelt. Sie kann vielmehr zu einer Bedrohung werden, wenn eine schädliche codierte Befehlszeile zum Einsatz kommt.

2. Klicken Sie auf die Schaltfläche **Ausnahme hinzufügen** am oberen Ende der Tabelle.
3. Wählen Sie im Konfigurationsfenster die Richtlinien, zu denen die Ausnahme hinzugefügt werden soll und klicken Sie anschließend auf **Hinzufügen**.

Informationen über die hinzugefügten Ausnahmen werden standardmäßig an die Bitdefender-Labs übermittelt, um die Erkennungsmöglichkeiten der Bitdefender-Produkte zu verbessern. Diese Option kann über das Kästchen

Übermitteln Sie dieses Feedback an Bitdefender für eine bessere Analyse ein- und ausgeschaltet werden.

Wenn die Bedrohung vom Malware-Schutz-Modul gefunden wurde, gilt die Ausnahme für Zugriff- und Bedarf-Scans.



Beachten Sie

Sie finden die Ausnahmen in den folgenden Bereichen der ausgewählten Richtlinien: **Malware-Schutz > Einstellungen** für Dateien und **Inhaltssteuerung > Datenverkehr** für URLs.

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Endpunkte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde. Sie können auch den Benutzer anzeigen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Endpunkte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Endpunkte ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Endpunkte mit behobener Malware (alle als infiziert erkannte Dateien wurden erfolgreich desinfiziert oder in die **Quarantäne** verschoben)
- Endpunkte mit nicht behobener Malware (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Für jeden Endpunkt können Sie die Liste der Bedrohungen und der betroffenen Dateipfade anzeigen, indem Sie in den Spalten der Desinfektionsergebnisse auf die entsprechenden Links klicken.

In diesem Bericht können Sie schnell einen vollständigen System-Scan auf den Zielen ausführen, auf denen noch keine Behebung durchgeführt wurde, indem Sie in der Symbolleiste über der Datentabelle auf die Schaltfläche **Infizierte Ziele scannen** klicken.

Netzwerkvorfälle

Informiert Sie über die Aktivitäten des Network Attack Defense-Moduls. Ein Diagramm zeigt die Anzahl der Angriffsversuche, die über einen bestimmten Zeitraum erkannt wurden. Die Berichtsdetails umfassen:

- Endpunktname, IP und FQDN
- Nutzernamen
- Name des Fundes

- Angriffstechnik
- Anzahl der Versuche
- IP des Angreifers
- Betroffene IP und Port
- Wann der Angriff zuletzt blockiert wurde

Wenn Sie bei einem Fund auf die Schaltfläche **Ausnahmen hinzufügen** klicken, wird automatisch ein Eintrag unter **Global Ausschlüsse** im Bereich **Netzwerkschutz** angelegt.

Patch-Status im Netzwerk

Prüfen Sie den Update-Status der in Ihrem Netzwerk installierten Software. Der Bericht liefert die folgenden Informationen:

- Zielmaschine (Endpunktname, IP und Betriebssystem).
- Sicherheitsrelevante Patches (installierte Patches, fehlgeschlagene Patches und nicht sicherheitsrelevante Patches).
- Status und Zeitpunkt der letzten Änderung für ausgecheckte Endpunkte.

Netzwerkschutzstatus

Zeigt detaillierte Information zum allgemeinen Sicherheitsstatus der Zielpunkte. Hier finden Sie zum Beispiel folgende Informationen:

- Name, IP und FQDN
- Status:
 - **Hat Probleme** - Auf dem Endpunkt gibt es Schutzlücken (Sicherheitsagent nicht auf dem neuesten Stand, Sicherheitsbedrohungen entdeckt usw.)
 - **Keine Probleme** - Der Endpunkt ist geschützt und es gibt keinen Grund zur Besorgnis.
 - **Unbekannt** - Der Endpunkt war zum Zeitpunkt der Berichterstellung offline.
 - **Nicht verwaltet** - Der Sicherheitsagent wurde bisher noch nicht auf dem Endpunkt installiert.
- Verfügbare [Sicherheitsebenen](#)
- Verwaltete und nicht verwaltete Endpunkte (Sicherheitsagent ist installiert oder nicht)

- Lizenztyp und -status (weitere Spalten mit Lizenzinformationen sind standardmäßig ausgeblendet)
- Infektionsstatus (der Endpunkt ist "sauber" oder nicht)
- Update-Status des Produkts und der Sicherheitsinhalte
- Software-Sicherheitspatch-Status (fehlende sicherheitsrelevante und nicht sicherheitsrelevante Patches)

Bei nicht verwalteten Endpunkten sehen Sie den Status **Nicht verwaltet** unter weiteren Spalten.

Prüfvorgang

Liefert Informationen zu den Bedarf-Scans, die auf den ausgewählten Zielen durchgeführt wurden. Eine Statistik der erfolgreichen und fehlgeschlagenen Scans wird in einem Kuchendiagramm angezeigt. In der Tabelle unter dem Diagramm werden Details zum Scan-Typ, zum letzten Auftreten und zum letzten erfolgreichen Scan für jeden Endpunkt angezeigt.

Richtlinienkonformität

Liefert Informationen zu den Sicherheitsrichtlinien, die auf den ausgewählten Zielen angewendet werden. Der Status der Richtlinie wird in einem Kuchendiagramm angezeigt. Der Tabelle unter der Grafik können Sie die jedem Endpunkt zugewiesene Richtlinie und den Richtlinientyp sowie das Datum und den zuweisenden Benutzer entnehmen.

Sandbox Analyzer – Fehlgeschlagene Übermittlungen

Zeigt alle fehlgeschlagenen Übermittlungen von Objekten an, die während eines bestimmten Zeitraums von den Endpunkten an den Sandbox Analyzer gesendet wurden. Eine Übermittlung gilt nach mehreren Versuchen als fehlgeschlagen.

In der Grafik wird die Variation der fehlgeschlagenen Übertragungen während des festgelegten Zeitraums dargestellt. In der Detailtabelle des Berichts werden die Dateien aufgeführt, die nicht an den Sandbox Analyzer gesendet werden konnten, außerdem die Maschine, von der aus das Objekt gesendet wurde, Datum und Uhrzeit jedes erneuten Versuchs, der zurückgegebene Fehlercode, die Beschreibung jedes fehlgeschlagenen Versuchs und der Unternehmensname.

Sandbox Analyzer-Ergebnisse (veraltet)

Liefert detaillierte Informationen zu den Dateien auf den entsprechenden Endpunkten, die in der Sandbox während eines bestimmten Zeitraums analysiert wurden. In einem Liniendiagramm wird die Anzahl der unbedenklichen und die


der gefährlichen analysierten Dateien angezeigt, und in einer Tabelle sind Details zu jedem Fall aufgeführt.

Sie können für alle analysierten Dateien oder nur für die als schädlich eingestufteten Dateien einen Sandbox Analyzer-Ergebnisbericht erstellen.

Sie können Folgendes sehen:

- Ergebnis der Analyse, also die Information, ob die Datei unbedenklich, gefährlich oder unbekannt (**Bedrohung gefunden** oder **Keine Bedrohung gefunden** oder **Nicht unterstützt**) ist. Diese Spalte wird nur angezeigt, wenn Sie im Bericht alle analysierten Objekte anzeigen lassen.

Eine vollständige Liste der vom Sandbox Analyzer unterstützten Dateitypen und -erweiterungen finden Sie hier: [„Unterstützte Dateitypen und Dateierweiterungen für die manuelle Übermittlung“](#) (S. 549).

- Bedrohungstyp, z. B. Adware, Rootkit, Downloader, Exploit, Host-Modifier, Schad-Tools, Passwort-Stehler, Ransomware, Spam oder Trojaner.
- Datum und Uhrzeit des Fundes, wonach Sie je nach Berichtszeitraum filtern können.
- Hostname oder IP-Adresse des Endpunkts, auf dem die Datei gefunden wurde.
- Name der Dateien, wenn sie einzeln übermittelt wurden, oder Anzahl der analysierten Dateien im Fall einer gebündelten Übermittlung. Wenn Sie auf den Dateinamen oder auf den Link des Bündels klicken, werden Details und ausgeführte Aktionen angezeigt.
- Status der Bereinigungsaktion für die übertragenen Dateien (**Teilweise, Fehlgeschlagen, Nur berichtet, Erfolgreich**).
- Unternehmensname.
- Weitere Informationen zu den Eigenschaften der analysierten Datei erhalten Sie, wenn Sie in der Spalte **Analyseergebnis** auf die Schaltfläche  **Mehr** klicken. Hier werden Sicherheitsaspekte und das Verhalten der untersuchten Datei im Detail angezeigt.

Der Sandbox Analyzer zeichnet die folgenden Ereignisse auf:

- Schreiben, Löschen, Verschieben, Kopieren, Ersetzen von Dateien im System und auf tragbaren Datenträgern.
- Ausführen von neu erstellten Dateien.
- Änderungen am Dateisystem.
- Änderungen an den laufenden Anwendungen innerhalb einer virtuellen Maschine.
- Änderungen an der Windows-Taskleiste und am Startmenü.

- Erstellen, Beenden, Injizieren von Prozessen.
- Schreiben oder Löschen von Registrierungsschlüsseln.
- Erstellen von Mutex-Objekten.
- Erstellen, Starten, Anhalten, Modifizieren, Abfragen, Löschen von Diensten.
- Ändern der Browser-Sicherheitseinstellungen.
- Änderung der Windows-Explorer-Anzeigeeinstellungen.
- Hinzufügen von Dateien zur Firewall-Ausnahmeliste.
- Änderung von Netzwerkeinstellungen.
- Aktivieren einer Ausführung beim Systemstart.
- Herstellen einer Verbindung zu einem entfernten Host.
- Zugriff auf bestimmte Domains.
- Transfer von Daten von und zu bestimmten Domains.
- Zugriff auf URLs, IP-Adressen und Ports über verschiedene Kommunikationsprotokolle.
- Überprüfen der Indikatoren virtueller Umgebungen.
- Überprüfen der Indikatoren von Überwachungstools.
- Erstellen von Bildschirm- oder Systemabbildern.
- SSDT, IDT, IRP-Hooks.
- Speicherabbilder für verdächtige Prozesse.
- Windows-API-Funktionsaufrufe.
- Wechsel in die Inaktivität für einen bestimmten Zeitraum zur Verzögerung der Ausführung.
- Erstellen von Dateien, die in bestimmten zeitlichen Intervallen auszuführende Aktionen beinhalten.

Klicken Sie im Fenster **Analyseergebnis** auf die Schaltfläche **Download**, um auf Ihrem Computer den Inhalt der Verhaltenszusammenfassung in einem der folgenden Formate zu speichern: XML, HTML, JSON, PDF.

Dieser Bericht wird noch eine begrenzte Zeit lang unterstützt. Es wird empfohlen, stattdessen Übermittlungskarten zu verwenden, um die notwendigen Informationen über die analysierten Stichproben zu sammeln. Sie finden die Übermittlungskarten im Abschnitt **Sandbox Analyzer** im Control Center-Hauptmenü.

Sicherheitsüberprüfung

Liefert Informationen zu Sicherheitsereignissen auf einem ausgewählten Ziel. Die Informationen beziehen sich auf die folgenden Ereignisse:

- Malware-Erkennung
- Blockierte Anwendung

- Blockierter Scan-Port
- Blockierter Datenverkehr
- Blockierte Website
- Gerät blockieren
- Blockierte E-Mail
- Blockierter Prozess
- HVI-Ereignisse
- Erweiterter Exploit-Schutz-Ereignisse
- Network Attack Defense-Ereignisanzeige
- Ransomware-Fund

Security Server-Status

Hiermit können Sie den Status eines Security Server bewerten. Verschiedene Statusindikatoren helfen Ihnen dabei, etwaige Probleme eines Security Server zu identifizieren:

- **Status:** Zeigt den allgemeinen Status des Security Servers an.
- **Maschinen-Status:** zeigt an, welche Security Server-Appliances angehalten wurden.
- **AV-Status:** zeigt an, ob das Malware-Schutz-Modul aktiviert oder deaktiviert ist.
- **Update-Status:** zeigt an, ob die Security Server-Appliances auf dem neuesten Stand sind oder ob Updates deaktiviert wurden.
- **Auslastungsstatus:** Zeigt den Scan-Auslastungsgrad eines Security Server wie hier beschrieben an:
 - **Unterbelastet**, wenn weniger als 5 % der Scan-Kapazität verwendet werden.
 - **Normal**, wenn die Scan-Last ausgeglichen ist.
 - **Überlastet**, wenn die Scan-Last 90 % ihrer Kapazität übersteigt. Überprüfen Sie in einem solchen Fall die Sicherheitsrichtlinien. Falls alle Security Server überlastet sind, die innerhalb einer Richtlinie zugeordnet wurden, müssen Sie der Liste einen weiteren Security Server hinzufügen. Überprüfen Sie andernfalls die Netzwerkverbindung zwischen den Clients und den Security Servern ohne Lastprobleme.
- **Mit HVI geschützte VMs:** Informiert Sie über virtuelle Maschinen, die mit dem HVI-Modul überwacht und geschützt werden.

- **HVI-Status:** Zeigt an, ob das Modul aktiviert oder deaktiviert ist. HVI wird aktiviert, wenn sowohl der Security Server als auch das Ergänzungspaket auf dem Host installiert sind.
- **Verbundene Speichergeräte:** informiert Sie darüber, wie viele ICAP-konforme Speichergeräte mit Security Server verbunden sind. Wenn Sie auf die Zahl klicken, wird die Liste der Speichergeräte mit Details zu jedem einzelnen angezeigt: Name, IP, Art, Datum und Zeitpunkt der letzten Verbindung.
- **Status des Speicher-Scans:** zeigt an, ob der Security for Storage-Dienst aktiviert oder deaktiviert ist.

Darüber hinaus können Sie die Anzahl der mit dem Security Server verbundenen Agenten einsehen. Mit einem Klick auf die Zahl der verbundenen Clients wird die Liste der Endpunkte angezeigt. Diese Endpunkte könnten für Angriffe anfällig sein, wenn Probleme mit dem Security Server auftreten.

Top-10 der gefundenen Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den ausgewählten Endpunkten gefunden wurden.



Beachten Sie

In der Detailtabelle werden alle Endpunkte angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Top-10 der infizierten Endpunkte

Zeigt von den ausgewählten Endpunkten die 10 mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.



Beachten Sie

In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Endpunkten gefunden wurde.

Update-Status

Zeigt Ihnen den Update-Status des auf ausgewählten Zielen installierten Sicherheitsagenten oder Security Server an. Der Update-Status bezieht sich auf das Produkt und die Versionen der Sicherheitsinhalte.

Über die verfügbaren Filter können Sie schnell feststellen, welche Clients in den letzten 24 Stunden aktualisiert und welche nicht aktualisiert wurden.

In diesem Bericht können Sie schnell die Agenten auf die neueste Version aktualisieren. Klicken Sie dazu in der Symbolleiste über der Datentabelle auf die Schaltfläche **Update**.

Upgrade-Status

Zeigt an, welche Sicherheitsagenten auf den ausgewählten Zielen installiert sind und ob es eine neuere Version dazu gibt.

Auf Endpunkten mit alten Sicherheitsagenten können Sie ganz einfach den neuesten unterstützten Sicherheitsagenten installieren, indem Sie auf die Schaltfläche **Upgrade durchführen** klicken.



Beachten Sie

Dieser Bericht steht nur zur Verfügung, wenn ein Upgrade für die GravityZone-Lösung durchgeführt wurde.

Sicherheitsstatus des Netzwerks virtueller Maschinen

Informiert Sie über die Abdeckung des Bitdefender-Schutzes in Ihrer virtualisierten Umgebung. Für jede der ausgewählten Maschinen können Sie anzeigen, welche Komponente die Sicherheitsprobleme behebt:

- Security Server für agentenlose Installationen in VMware-NSX- und vShield-Umgebungen und für HVI
- Ein Sicherheitsagenten in allen anderen Fällen

HVI Aktivität

Informiert Sie über alle Angriffe, die die HVI-Module auf den ausgewählten Maschinen innerhalb eines bestimmten Zeitraums erkannt haben.

Der Bericht beinhaltet auch Informationen über Datum und Uhrzeit des letzten erkannten Vorfalls im überwachten Prozess, den Abschlussstatus der gegen den Angriff unternommenen Maßnahme, den Benutzer zum Zeitpunkt des Prozessstarts sowie die entsprechende Maschine.

Abhängig von der ergriffenen Maßnahme kann der gleiche Vorgang mehrmals gemeldet werden. Wenn zum Beispiel ein Prozess einmal beendet und ein anderes Mal der Zugang verweigert wurde, erscheinen zwei Einträge in der Berichtstabelle.

Beim Klicken auf das Datum des letzten Funds wird für jeden Prozess ein separater Eintrag mit allen erkannten Vorfällen seit Prozessstart angezeigt. Der Eintrag enthält wichtige Informationen wie z.B. Art und Beschreibung des Vorfalls, Quelle und Ziel des Angriffs und Maßnahmen zur Beseitigung des Problems.

In diesem Bericht können Sie das Sicherheitsmodul anweisen, bestimmte Ereignisse zu ignorieren, die Sie als legitim einstufen. Klicken Sie dazu in der Symbolleiste über der Datentabelle auf die Schaltfläche **Ausnahme hinzufügen**.



Beachten Sie

Das HVI-Module ist in einigen GravityZone-Lösungen über einen separaten Lizenzschlüssel erhältlich.

HVI-Drittanbieter-Tool-Injektionsstatus

Hier erhalten Sie eine detaillierte Statusübersicht für jede auf den Zielpunkten durchgeführte Injektion. Angezeigt wird:

- Der Name des Endpunktes.
- Der Name des injizierten Tools.
- Die IP-Adresse des Endpunktes.
- Das Gast-Betriebssystem.
- Der Auslöser. Hierbei kann es sich um eine Speicherverletzung, eine Bedarf-Aufgabe oder einen geplanten Ausführung handeln.
- Die Anzahl der erfolgreichen Ausführungen. Klicken Sie auf die Zahl, um ein Fenster mit den Protokollpfaden und einen Zeitstempel für jede Tool-Ausführung zu öffnen. Mit einem Klick auf das Symbol vor dem Pfad wird eine Kopie in die Zwischenablage gelegt.
- Die Anzahl der fehlgeschlagenen Ausführungen. Klicken Sie auf die Zahl, um ein Fenster mit den Grund für das Fehlschlagen und einen Zeitstempel zu öffnen.
- Letzte erfolgreiche Injektion.

Injektionen werden nach Zielpunkten geordnet. Sie können über die Filteroptionen in der Kopfzeile der Tabelle auf den Bericht Filter anwenden, um nur Daten zu einem bestimmten Tool anzuzeigen.

Ransomware-Aktivität

Informiert Sie über die Ransomware-Angriffe, die GravityZone auf den von Ihnen verwalteten Endpunkten erkannt hat, und stellt Ihnen die erforderlichen Tools zur Verfügung, um die von den Angriffen betroffenen Dateien wiederherzustellen.

Anders als andere Berichte ist der Bericht als eigene Seite im Control Center verfügbar und kann direkt über das GravityZone-Hauptmenü aufgerufen werden.

Die Seite **Ransomware-Aktivität** besteht aus einem Raster, das für jeden Ransomware-Angriff folgende Informationen anzeigt:

- Name, IP-Adresse und FQDN des Endpunkts, auf dem der Angriff stattfand
- Das Unternehmen, zu dem der Endpunkt gehört
- Der Name des Benutzers, der während des Angriffs angemeldet war
- Der Angriffstyp, d. h. lokal oder remote
- Der Prozess, unter dem die Ransomware bei lokalen Angriffen ausgeführt wurde bzw. die IP-Adresse, von der aus der Angriff bei Remote-Angriffen gestartet wurde
- Datum und Uhrzeit des Fundes
- Anzahl der Dateien, die verschlüsselt wurden, bis der Angriff blockiert wurde
- Der Status der Wiederherstellungsaktion für alle Dateien auf dem Zielendpunkt

Einige Details werden standardmäßig ausgeblendet. Klicken Sie auf die Schaltfläche **Spalten ein-/ausblenden** oben rechts auf der Seite, um die Details zu konfigurieren, die Sie im Raster anzeigen möchten. Wenn Sie viele Einträge im Raster haben, können Sie Filter über die Schaltfläche **Filter ein-/ausblenden** oben rechts auf der Seite ausblenden.

Weitere Informationen erhalten Sie durch Anklicken der Anzahl der Dateien. Sie können eine Liste mit dem vollständigen Pfad zu den ursprünglichen und wiederhergestellten Dateien sowie den Wiederherstellungsstatus für alle an dem ausgewählten Ransomware-Angriff beteiligten Dateien anzeigen.



Wichtig

Die Sicherungskopien sind maximal 30 Tage lang verfügbar. Bitte achten Sie auf das Datum und die Uhrzeit, zu denen die Dateien noch wiederhergestellt werden können.

So können Sie von Ransomware betroffenen Dateien wieder herstellen:

1. Wählen Sie die Angriffe aus, die im Raster aufgeführt werden sollen.
2. Klicken Sie auf **Dateien wiederherstellen**. Ein Bestätigungsfenster wird angezeigt.

Es wird eine Wiederherstellungsaufgabe erstellt. Sie können ihren Status wie bei jeder anderen Aufgabe in GravityZone auf der Seite **Aufgaben** einsehen.

Wenn Funde das Ergebnis harmloser Prozesse sind, gehen Sie wie folgt vor:

1. Wählen Sie die Datensätze im Raster aus.
2. Klicken Sie auf die Schaltfläche **Ausschluss hinzufügen**.
3. Wählen Sie im neuen Fenster die Richtlinien aus, für die der Ausschluss gelten soll.
4. Klicken Sie auf **Hinzufügen**.

wird alle möglichen Ausschlüsse anwenden: auf den Ordner, auf den Prozess und auf die IP-Adresse.

Sie können sie im Richtlinienabschnitt **Malware-Schutz > Einstellungen > Benutzerdefinierte Ausschlüsse** überprüfen oder anpassen.



Beachten Sie

Ransomware-Aktivität zeichnet Ereignisse zwei Jahre lange auf.

9.1.2. Exchange-Server-Berichte

Die folgenden Arten von Berichten sind für Exchange-Server verfügbar:

Exchange - Blockierte Inhalte und Anhänge

Enthält Informationen über E-Mails oder Anhänge, die von der Inhaltssteuerung während eines bestimmten Zeitraums von den ausgewählten Servern gelöscht wurden. Angezeigt wird:

- E-Mail-Adressen des Absenders und der Empfänger.
Wenn die E-Mail mehrere Empfänger hat, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.
- E-Mail-Betreff.
- Erkennungstyp; zeigt an, von welchem Inhaltssteuerungsfilter die Bedrohung gefunden wurde.
- Die durchgeführte Aktion.
- Der Server, auf dem die Bedrohung gefunden wurde.

Exchange – blockierte unscannbare Anhänge

Enthält Informationen zu E-Mails mit nicht scanbaren Anhängen (überkomprimiert, passwortgeschützt usw.), die auf den ausgewählten Exchange-Mail-Servern über einen bestimmten Zeitraum blockiert wurden. Die Informationen beziehen sich auf:

- E-Mail-Adressen des Absenders und der Empfänger.

Wenn die E-Mail an mehrere Empfänger gesendet wurde, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.

- E-Mail-Betreff.
- Zur Entfernung von nicht scanbaren Anhängen durchgeführte Aktionen:
 - **Gelöschte E-Mail** zeigt an, dass die gesamte E-Mail entfernt wurde.
 - **Gelöschte Anhänge** allgemeine Bezeichnung für alle Aktionen, bei denen Anhänge aus einer E-Mail-Nachricht entfernt werden, so zum Beispiel durch Löschen des Anhangs, durch Verschieben in die Quarantäne oder durch Austausch mit einer Benachrichtigung.

Mit einem Klick auf den Link in der Spalte **Aktion** können Sie Details zu jedem blockierten Anhang und die jeweils durchgeführte Aktion anzeigen.

- Zeitpunkt des Fundes.
- Der Server, auf dem die E-Mail gefunden wurde.

Exchange - E-Mail-Scan-Aktivität

Zeigt Statistiken zu den vom Exchange-Schutz-Modul während eines bestimmten Zeitraums durchgeführten Aktionen an.

Die Aktionen werden nach Typ (Malware, Spam, unzulässiger Anhang und unzulässiger Inhalt) und nach Server zu Gruppen zusammengefasst.

Die Statistiken beziehen sich auf die folgenden E-Mail-Status:

- **In Quarantäne.** Diese E-Mails wurden in den Quarantäne-Ordner verschoben.
- **Gelöscht/Abgelehnt.** Diese E-Mails wurden vom Server gelöscht oder abgelehnt.
- **Umgeleitet.** Diese E-Mails wurden an die in der Richtlinie angegebene E-Mail-Adresse umgeleitet.

- **Bereinigt und zugestellt.** Diese E-Mails wurden von den Filtern durchgelassen, nachdem Bedrohungen entfernt worden sind.
Eine E-Mail gilt als bereinigt, wenn alle als potenziell schädlich erkannten Anhänge desinfiziert, in die Quarantäne verschoben, gelöscht oder durch Text ersetzt wurden.
- **Geändert und zugestellt.** Diese E-Mails wurden von den Filtern durchgelassen, nach dem Scan-Informationen den E-Mail-Headern hinzugefügt wurden.
- **Ohne weitere Aktion zugestellt.** Diese E-Mails wurden vom Exchange-Schutz ignoriert und von den Filtern durchgelassen.

Exchange - Malware-Aktivität

Enthält Informationen über E-Mails mit Malware-Bedrohungen, die in einem bestimmten Zeitraum auf den ausgewählten Exchange-Mail-Servern gefunden wurden. Die Informationen beziehen sich auf:

- E-Mail-Adressen des Absenders und der Empfänger.
Wenn die E-Mail an mehrere Empfänger gesendet wurde, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.
- E-Mail-Betreff.
- E-Mail-Status nach Malware-Scan.
Mit einem Klick auf den Status-Link werden Details zur gefundenen Malware und der durchgeführten Aktion angezeigt.
- Zeitpunkt des Fundes.
- Der Server, auf dem die Bedrohung gefunden wurde.

Exchange - Top-10 der gefundenen Malware

Zeigt die 10 am häufigsten in E-Mail-Anhängen gefundenen Malware-Bedrohungen. Sie können zwei verschiedene Ansichten mit unterschiedlichen Statistiken generieren. Die eine zeigt die Anzahl der Funde nach betroffenen Empfängern, die andere nach Absendern an.

Nehmen wir an, GravityZone hat eine E-Mail mit infiziertem Anhang gefunden, die an fünf Empfänger gesendet wurde.

- In der Empfängeransicht:
 - Der Bericht zeigt fünf Funde.

- In den Berichtdetails werden nur die Empfänger, nicht die Absender, angezeigt.
- In der Absenderansicht:
 - Der Bericht zeigt einen Fund.
 - In den Berichtdetails wird nur der Absender, nicht die Empfänger, angezeigt.

Außer dem Namen der Malware und dem des Absenders/Empfängers enthält der Bericht die folgenden Informationen:

- Malware-Typ (Virus, Spyware, PUA, usw.)
- Der Server, auf dem die Bedrohung gefunden wurde.
- Maßnahmen, die das Malware-Schutz-Modul ergriffen hat.
- Zeitpunkt des letzten Fundes.

Exchange - Top-10 der Malware-Empfänger

Zeigt die 10 E-Mail-Empfänger an, die während eines bestimmten Zeitraums am häufigsten das Ziel von Malware waren.

In den Berichtdetails wird die gesamte Liste der Malware aufgeführt, die diese Empfänger betraf, zusammen mit den durchgeführten Aktionen.

Exchange - Top-10 der Spam-Empfänger

Zeigt die 10 E-Mail-Empfänger an, die in einem bestimmten Zeitraum die meisten erkannten Spam- oder Phishing-E-Mails empfangen haben. Im Bericht werden auch die Aktionen aufgeführt, die für diese E-Mails durchgeführt wurden.

9.1.3. Berichte zu Mobilgeräten



Beachten Sie

Malware-Schutz und damit verbundene Berichte stehen nur für Android-Geräte zur Verfügung.

Für Mobilgeräte stehen die folgenden Berichtstypen zur Verfügung:

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der mobilen Zielgeräte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde. Mobil Geräte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Mobilgeräte ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Mobilgeräte mit behobener Malware (alle gefundenen Dateien wurden entfernt)
- Mobilgeräte mit bestehender Malware (einige der gefundenen Dateien wurden nicht gelöscht)

Top-10 der infizierten Geräte

Zeigt von den mobilen Zielgeräten die 10 Geräte mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.



Beachten Sie

In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Mobilgeräte gefunden wurde.

Top-10 der gefundenen Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den mobilen Zielgeräten erkannt wurden.



Beachten Sie

In der Detailtabelle werden alle Mobilgeräte angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Gerätekonformität

Informiert Sie über den Konformitätsstatus der mobilen Zielgeräte. Hier sehen Sie den Namen, den Status, das Betriebssystem und den Grund für die Nichtkonformität des Geräts.

Weitere Informationen zu Konformitätsanforderungen finden Sie unter [„Kriterien für Nichtkonformität“](#) (S. 417).

Gerätesynchronisation

Informiert Sie über den Synchronisationsstatus der mobilen Zielgeräte. Hier können Sie den Namen des Geräts, den zugewiesenen Benutzer, den Synchronisationsstatus, das Betriebssystem und den Zeitpunkt, zu dem das Gerät zuletzt online gesehen wurde einsehen.

Weitere Informationen finden Sie unter [„Status der Mobilgeräte überprüfen“](#) (S. 179).

Blockierte Webseiten

Informiert Sie über die Anzahl der Versuche der Zielgeräte, über einen bestimmten Zeitraum auf Websites zuzugreifen, die durch **Internetzugangsregeln** blockiert wurden.

Bei Funden auf einen Gerät können Sie auf die Nummer in der Spalte **Blockierte Websites** klicken, um detaillierte Informationen für jede blockierte Webseite anzuzeigen, so zum Beispiel:

- URL
- Richtlinienkomponente, die die Aktion vorgenommen hat
- Anzahl blockierter Versuche
- Zeitpunkt, zu dem die Website zuletzt blockiert wurde

Weitere Informationen zu den Richtlinienereinstellungen für den Internetzugang finden Sie unter „[Profile](#)“ (S. 422).

Web-Sicherheit-Aktivität

Informiert Sie über die Anzahl der Versuche der Zielgeräte, über einen bestimmten Zeitraum auf Websites mit Sicherheitsbedrohungen (Phishing, Betrug, Malware oder unsichere Websites) zuzugreifen. Bei Funden auf einen Gerät können Sie auf die Nummer in der Spalte **Blockierte Websites** klicken, um detaillierte Informationen für jede blockierte Webseite anzuzeigen, so zum Beispiel:

- URL
- Art der Bedrohung (Phishing, Malware, Betrug, unsicher)
- Anzahl blockierter Versuche
- Zeitpunkt, zu dem die Website zuletzt blockiert wurde

Web-Sicherheit ist die Richtlinienkomponente, die Websites mit Sicherheitsproblemen erkennt und blockiert. Weitere Informationen zu den Richtlinienereinstellungen für die Web-Sicherheit finden Sie unter „[Sicherheit](#)“ (S. 412).

9.2. Berichte erstellen

Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **Sofortberichte.** Sofortberichte werden automatisch angezeigt, sobald sie erstellt wurden.

- **Geplante Berichte.** Berichte können so geplant werden, dass sie in regelmäßigen Abständen und/oder zu einem bestimmten Zeitpunkt erstellt werden. Eine Liste aller geplanten Berichte finden Sie auf der Seite **Berichte**.

**Wichtig**

Sofortberichte werden automatisch gelöscht, wenn Sie die Berichtsseite schließen. Geplante Berichte werden auf der Seite **Berichte** gespeichert und angezeigt.

Um einen Bericht zu erstellen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Netzwerkobjekttyp aus der [Ansichtsauswahl](#).
3. Klicken Sie auf die Schaltfläche **+Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.

Bericht erstellen
✕

Details

Typ:

Name: *

Einstellungen

Jetzt
 Geplant

Berichtsintervall:

Anzeigen: Alle Endpunkte
 Nur Endpunkte mit blockierten Websites

Zustellung: Per E-Mail senden an

Ziel auswählen

Computer und virtuelle Maschinen

Ausgewählte Gruppen

Generieren
Abbrechen

Optionen für Berichte zu Computern und virtuellen Maschinen

4. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus. Weitere Informationen finden Sie unter „Berichtstypen“ (S. 438)
5. Geben Sie einen eindeutigen Namen für den Bericht ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen.
6. Konfigurieren Sie die Wiederholung des Berichts:
 - Mit **Jetzt** erstellen Sie einen Sofortbericht.

- Mit **Geplant** können Sie den Bericht so konfigurieren, dass er regelmäßig nach einem gewünschten Intervall generiert wird:
 - Stündlich. Immer nach einer festgelegten Anzahl von Stunden.
 - Täglich. Hierbei können Sie auch die Startzeit (Stunde und Minute) festlegen.
 - Wöchentlich, am festgelegten Wochentag zur festgelegten Startzeit (Stunde und Minute).
 - Monatlich, am festgelegten Tag des Monats zur festgelegten Startzeit (Stunde und Minute).
7. Für die meisten Berichtstypen müssen Sie das Intervall angeben, auf das sich die im Bericht enthaltenen Daten beziehen. Der Bericht zeigt nur Daten aus dem gewählten Zeitraum an.
 8. Viele Berichtsarten enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Verwenden Sie die Filtermöglichkeiten im Bereich **Anzeigen**, um nur die gewünschten Informationen abzurufen.

Für einen **Update-Status**-Bericht können Sie zum Beispiel auf Wunsch nur die Netzwerkobjekte anzeigen, die nicht aktualisiert wurden, oder diejenigen, die neu gestartet werden müssen, um das Update abzuschließen.
 9. **Zustellung**. Um einen geplanten Bericht als E-Mail geschickt zu bekommen, markieren Sie das entsprechende Kästchen. Geben Sie die gewünschten E-Mail-Adresse in das Feld darunter ein. Die E-Mail enthält standardmäßig ein Archiv mit beiden Berichtdateien (PDF und CSV). Über die Kästchen im Bereich **Dateien anhängen** können Sie festlegen, welche Dateien per E-Mail versandt werden sollen und wie.
 10. **Ziel auswählen**. Scrollen Sie nach unten, das Ziel des Berichts zu konfigurieren. Wählen Sie eine oder mehrere Gruppen von Endpunkten, die Sie in den Bericht einbeziehen möchten.
 11. Klicken Sie je nach Wiederholungsintervall auf **Generieren**, um einen Sofortbericht zu erstellen, oder auf **Speichern**, um einen geplanten Bericht zu erstellen.
 - Ein Sofortbericht wird sofort angezeigt, nachdem Sie auf **Generieren** klicken. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von

der Anzahl der verwalteten Netzwerkobjekte ab. Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.

- Der geplante Bericht wird in der Liste auf der Seite **Berichte** angezeigt. Nachdem eine Berichtsinstanz generiert wurde, können Sie den Bericht anzeigen, indem Sie auf den entsprechenden Link in der Spalte **Bericht anzeigen** auf der Seite **Berichte** klicken.

9.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.

	Berichtsname	Typ	Wiederholung	Bericht anzeigen
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	Malware-Aktivitätsbericht	Malware-Aktivität	Täglich	Es wurde noch kein Bericht generiert

Die Berichteseite

Alle geplanten Berichte werden zusammen mit nützlichen Informationen zu den Berichten in einer Tabelle angezeigt:

- Name und Art des Berichts
- Berichtswiederholung
- Zuletzt generierte Instanz



Beachten Sie

Geplante Berichte sind nur für den Benutzer verfügbar, der diese auch erstellt hat.

Um Berichte nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Sie können das Suchfeld leeren, indem Sie mit dem Mauszeiger darüber fahren und auf das **×** **Löschen**Symbol klicken.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **☺ Neu laden**.

9.3.1. Berichte betrachten

So zeigen Sie einen Bericht an:

1. Gehen Sie zur Seite **Berichte**.
2. Sortieren Sie die Berichte nach Namen, Typ oder Wiederholung, um den gewünschten Bericht leichter zu finden.
3. Klicken Sie in der Spalte **Bericht anschauen** auf den entsprechenden Link, um den Bericht anzuzeigen. Die jüngste Berichtsinstanz wird angezeigt.

Wie Sie alle Instanzen eines Berichts anzeigen, erfahren Sie unter „[Berichte speichern](#)“ (S. 467)

Alle Berichte haben eine Zusammenfassungsteil (die obere Hälfte der Berichtsseite) und einen Detailsteil (die untere Hälfte der Berichtsseite).

- Der Zusammenfassungsbereich enthält statistische Daten (Kuchendiagramme und Grafiken) für alle Netzwerkobjekte sowie allgemeine Informationen über den Bericht wie den Berichtszeitraum (sofern anwendbar), Berichtsziel, usw.
- Der Detailbereich enthält Informationen zu allen entsprechenden Netzwerkobjekten.



Beachten Sie

- Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden.
- Klicken Sie auf den Bereich der Grafik (Kuchensegment oder Balken), der Sie interessiert, um in der Tabelle Details dazu anzuzeigen.

9.3.2. Geplante Berichte bearbeiten



Beachten Sie

Wenn Sie einen geplanten Bericht bearbeiten, werden sämtliche Änderungen mit der nächsten Ausführung des Berichts wirksam. Zuvor erstellte Berichte sind von den Änderungen nicht betroffen.

Um die Einstellungen eines geplanten Berichts zu ändern:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf den Berichtnamen.
3. Ändern Sie die Berichtseinstellungen nach Bedarf. Sie können die folgenden Änderungen vornehmen:
 - **Berichtsname.** Geben Sie dem Bericht einen eindeutigen Namen, der seinen Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen. Berichte die anhand eines geplanten Berichts erstellt werden, erhalten auch den entsprechenden Namen.
 - **Berichtswiederholung (geplant).** Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
 - **Einstellungen**
 - Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.


- Der Bericht wird nur Daten aus dem ausgewählten Intervall enthalten. Sie können das Intervall ab der nächsten Ausführung ändern.
- Die meisten Berichte enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Wenn Sie den Bericht in der Konsole anzeigen, sind unabhängig von den gewählten Optionen immer alle Informationen verfügbar. Wenn Sie den Bericht herunterladen oder per E-Mail versenden, werden nur die Berichtszusammenfassung und die ausgewählten Informationen in der PDF-Datei enthalten sein. Die Berichtsdetails sind nur im CSV-Format verfügbar.
- Sie können den Bericht auch per E-Mail erhalten.
- **Ziel wählen.** Die ausgewählte Option weist auf die Art des aktuellen Berichtsziels hin (entweder Gruppen oder einzelne Netzwerkobjekte). Klicken Sie auf den entsprechenden Link, um das aktuelle Berichtsziel anzuzeigen. Sie können das Berichtsziel ändern, indem Sie die Gruppen oder Netzwerkobjekte auswählen, die in dem Bericht eingeschlossen werden sollen.

4. Klicken Sie **Speichern**, um die Änderungen zu speichern.

9.3.3. Geplante Berichte löschen

Wenn ein geplanter Bericht nicht mehr benötigt wird, empfiehlt es sich, diesen zu löschen. Durch das Löschen eines geplanten Berichts werden alle Instanzen, die dieser bis zu diesem Zeitpunkt automatisch erstellt hat, gelöscht.

Um einen geplanten Bericht zu löschen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle.

9.4. Berichtsbasierte Aktionen ausführen

Die meisten Berichte stellen nur Probleme in Ihrem Netzwerk dar, manche geben Ihnen jedoch auch einige Optionen an die Hand, um diese Probleme mit ein paar einfachen Klicks zu beheben.

Wenn Sie die im Bericht dargestellten Probleme lösen möchten, können Sie dazu einfach auf die entsprechende Schaltfläche in der Symbolleiste über der Tabelle klicken.



Beachten Sie

Sie benötigen **Netzwerk verwalten**-Rechte, um diese Aktionen auszuführen.

Für jeden Bericht stehen die folgenden Optionen zur Verfügung:

Blockierte Anwendungen

- **Ausnahme hinzufügen.** Fügt einen Ausschluss in der Richtlinie hinzu, um zu verhindern, dass die Sicherheitsmodule die Anwendung noch einmal blockieren.
- **Regel hinzufügen.** Definiert eine Regel für eine Anwendung oder einen Prozess in der Anwendungssteuerung.

HVI Aktivität

- **Ausnahme hinzufügen.** Fügt einen Ausschluss in der Richtlinie hinzu, um zu verhindern, dass das Sicherheitsmodul den Vorfall noch einmal meldet.

Malware-Status

- **Infizierte Ziele scannen.** Führt einen vorkonfigurierten vollständigen Scan derjenigen Ziele aus, die als infiziert angezeigt werden.

Update-Status

- **Update.** Aktualisiert die entsprechenden Clients auf die neueste verfügbare Version.

Upgrade-Status

- **Upgrade durchführen.** Ersetzt alte Endpunkt-Clients durch die neuesten verfügbaren Produkte.

9.5. Berichte speichern

Standardmäßig werden geplante Berichte automatisch im Control Center gespeichert.

Wenn Sie Berichte über einen längeren Zeitraum hin benötigen, können Sie sie auf Ihrem Computer abspeichern. Die Zusammenfassung des Berichts ist im PDF-Format verfügbar; die Berichtsdetails sind jedoch nur im CSV-Format verfügbar.

Sie können Berichte auf zweierlei Weise speichern:

- [Exportieren](#)
- [Download](#)

9.5.1. Berichte exportieren


So exportieren Sie den Bericht auf Ihren Computer:

1. Klicken Sie je nach gewünschtem Format auf **CSV exportieren** oder **PDF exportieren**.
2. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

9.5.2. Berichte herunterladen

Einen Berichtsarchiv enthält sowohl die Zusammenfassung als auch die Details eines Berichts.

So laden Sie ein Berichtsarchiv herunter:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, den Sie speichern möchten.
3. Klicken Sie auf die Schaltfläche  **Herunterladen** und wählen Sie entweder **Letzte Instanz**, um die zuletzt erstellte Instanz des Berichts herunterzuladen, oder **Vollständiges Archiv**, um ein Archiv herunterzuladen, das sämtliche Instanzen enthält.

Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

9.6. Berichte per E-Mail versenden

Sie können Berichte mit den folgenden Optionen per E-Mail versenden:

1. Wenn Sie den angezeigten Bericht direkt per E-Mail versenden möchten, klicken Sie auf die Schaltfläche **E-Mail**. Der Bericht wird an die mit Ihrem Konto verknüpfte E-Mail-Adresse gesendet.
2. So konfigurieren Sie den Versand geplanter Berichte per E-Mail:
 - a. Gehen Sie zur Seite **Berichte**.
 - b. Klicken Sie auf den gewünschten Berichtsnamen.
 - c. Unter **Einstellungen > Zustellung Per Email senden an** auswählen.

- d. Geben Sie die gewünschte E-Mail-Adresse im Feld darunter ein. Sie können beliebig viele E-Mail-Adressen hinzufügen.
- e. Klicken Sie auf **Speichern**.

**Beachten Sie**

In der PDF-Datei, die per E-Mail gesendet wird, sind nur die Berichtszusammenfassung und das Diagramm enthalten. Die Berichtsdetails sind in der CSV-Datei enthalten.

Berichte werden als ZIP-Archive per E-Mail gesendet.

9.7. Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen. Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

9.8. Report-Builder

In Control Center können Sie Abfragen erstellen oder verwalten, mit deren Hilfe Sie jederzeit detaillierte Berichte über Ereignisse oder Änderungen in Ihrem Netzwerk erhalten.

Abfragen geben Ihnen die Möglichkeit, mithilfe unterschiedlicher Kriterien ein Sicherheitsproblem präzise und systematisch zu untersuchen. Mit Filtern können Sie Endpunkte nach bestimmten Kriterien gruppieren und relevante Daten zweckgerichtet auswählen.

Einem abfragebasierten Bericht können Sie Informationen entnehmen, wie z.B. Zeitpunkt eines Ereignisses, Anzahl der betroffenen Endpunkte, eingeloggte Nutzer zur Zeit des Vorfalls, Status des Sicherheitsagenten und an einem oder einer Gruppe von Endpunkten getroffene Maßnahmen.

Alle abfragebasierte Berichte stehen in Control Center zur Verfügung, Sie können sie aber auch in Ihrem Computer speichern oder per E-Mail versenden. Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

Durch Abfragen kommen Sie, im Vergleich zu GravityZone-Standardberichten, in den Genuss zahlreicher Vorteile:

- Zugriff auf große Datenmengen zum Erstellen aussagefähiger Berichte.
- Flexible Berichterstattung, da Ereignisse nicht zusammengefasst werden.

- Hoher Anpassungsgrad. Während GravityZone-Standardberichte Ihnen die Möglichkeit bieten, aus verschiedenen vordefinierten Optionen zu wählen, steht Ihnen mit Abfragen eine quasi unbegrenzte Anzahl an Datenfiltern zur Verfügung.
- Ereigniskorrelation, wobei die Informationen auch Daten über den Agenten und den Gerätestatus enthalten.
- Minimaler Entwicklungsaufwand, da Sie jeden Berichtstypus generieren, sichern und wieder verwenden können.
- Ausführliche Berichte, bei denen anders als bei Standardberichten Zusammenfassung und Details im gleichen PDF-Dokument enthalten sind.
- Abfragen können Information aus den letzten zwei Jahren abrufen.

Um Abfragen verwenden zu können, müssen Sie außer Ihrer virtuellen GravityZone-Appliance auch die Report-Builder-Rolle installieren. Ausführliche Informationen zur Installation von Report-Builder finden Sie in der GravityZone-Installationsanleitung.

9.8.1. Abfragetypen

GravityZone enthält die folgenden Abfragetypen:

- [Endpunkt-Status](#)
- [Endpunkt-Ereignisse](#)
- [Exchange-Ereignisse](#)

Endpunkt-Status

Über diese Abfrage erhalten Sie Informationen über den Sicherheitsstatus ausgewählter Ziel-Endpunkte für einen bestimmten Tag. So wissen Sie, ob der Sicherheitsagent und die Sicherheitsinhalte auf dem neusten Stand, veraltet oder deaktiviert sind. Zudem können Sie sehen, ob die Endpunkte infiziert oder bereinigt sind, welche Infrastruktur verwendet wird und welche Module an oder aus bzw. nicht installiert sind.

Diese Abfrage enthält Angaben zu den Ziel-Endpunkten, wie z.B.:

- Art der Maschine (physisch, virtuell oder Security Server)
- Netzwerkinfrastruktur, zu der der Endpunkt gehört (Active Directory, Nutanix Prism, VMWare oder Citrix Xen)
- Angaben zum Sicherheitsagenten (Typ, Status, Scan-Maschinenkonfiguration, Sicherheitsstatus)

- Sicherheitsmodul-Status
- Endpunkt-Rollen (Relay, Exchange-Schutz)

Endpunkt-Ereignisse

Mit dieser Abfrage können Sie Details über Sicherheitsereignisse auf den Ziel-Endpunkten für einen bestimmten Tag oder einen bestimmten Zeitraum abrufen. Sie enthält Informationen über:

- Die Zielmaschine, auf der das Ereignis stattfand (Name, Typ, IP, OS, Netzwerkinfrastruktur)
- Typ, Status und Konfiguration des installierten Sicherheitsagenten
- Status der auf dem Sicherheitsagenten installierten Schutz-Module und Rollen
- Name und Zuweisung der Richtlinie
- Eingeloggter Benutzer während des Ereignisses
- Ereignisse, die sich auf blockierte Webseiten, blockierte Anwendungen, Schadsoftware-Erkennung oder Geräteaktivität beziehen können

Exchange-Ereignisse

Hilft Ihnen, Ereignisse aufzufinden, die auf den ausgewählten Microsoft-Exchange-Servern an einem bestimmten Tag oder in einem bestimmten Zeitraum vorgefallen sind. Hierin sind folgende Daten berücksichtigt:

- Richtung des E-Mail-Datenverkehrs
- Sicherheitsereignisse (wie Erkennung von Schadsoftware oder schädlichem Anhang)
- In der jeweiligen Situation getroffene Maßnahme (Datei desinfiziert, gelöscht, ersetzt oder in Quarantäne verschoben bzw. E-Mail gelöscht oder abgewiesen)

9.8.2. Abfragen verwalten

Über die Seite **Bericht > Abfragen** können Sie Abfragen bzw. abfragebasierte Berichte generieren oder verwalten.



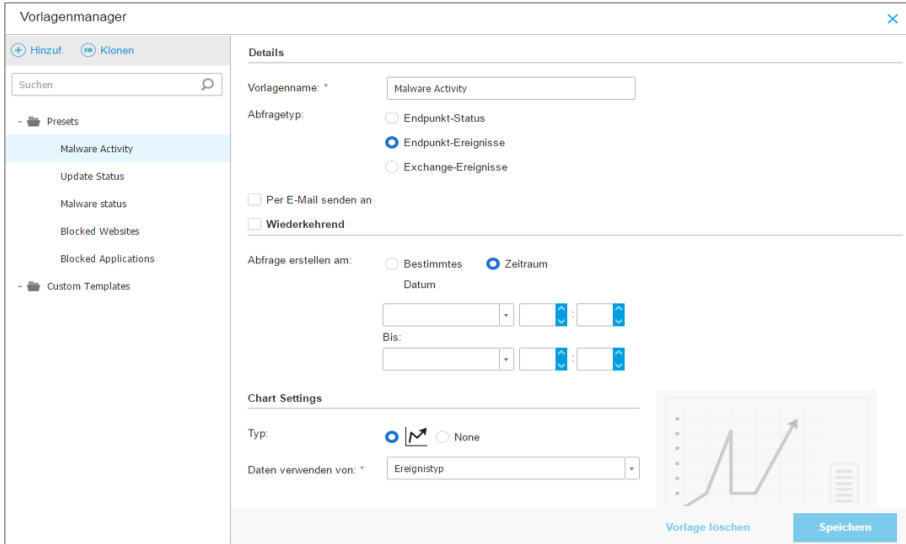
Name	Typ	Erstellt am	Berichtszeitraum	Suchanfrage
<input type="checkbox"/> Malware Activity	Endpunkt-Ereignisse	27 Sep 2016	1 Sep 2016-26 Sep 2016	
<input type="checkbox"/> Update Status	Endpunkt-Status	27 Sep 2016	27 Sep 2016-27 Sep 2016	
<input checked="" type="checkbox"/> Malware status	Endpunkt-Ereignisse	Nöch nicht generiert	Täglich	
<input type="checkbox"/> Blocked Websites	Endpunkt-Ereignisse	27 Sep 2016	1 Aug 2016-26 Sep 2016	
<input type="checkbox"/> Blocked Applications	Endpunkt-Ereignisse	27 Sep 2016	1 Sep 2016-26 Sep 2016	

Die Abfrage-Seite

Abfragen sind komplexe Zugriffe auf die Datenbasis unter Verwendung zahlreicher Filter, und es kann einige Minuten in Anspruch nehmen, sie zu erstellen und zu konfigurieren. Es kann frustrierend sein, jedes Mal das Abfrageformular auszufüllen, wenn ein neuer Bericht mit ähnlichen Merkmalen wie in früheren Berichten erstellt werden soll. GravityZone hilft Ihnen, Abfragen ganz einfach mit Hilfe von Vorlagen zu erstellen, die das Abfrageformular automatisch ausfüllen und so den Aufwand für Sie gering halten.

Vorlagen verwenden

Im Fenster **Vorlagen-Manager** können Sie Vorlagen hinzufügen, kopieren oder bestimmte Vorlagen mittels Schnellsuche finden.



Anzeige der verfügbaren Abfrage-Vorlagen:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie auf die Schaltfläche **Vorlagen** am oberen Rand der Tabelle. Das Fenster **Vorlagen-Manager** wird angezeigt. Alle Vorlagen werden im linken Fenster angezeigt, während Sie rechts die Einstellungen der ausgewählten Vorlage sehen können.

Zum schnellen Auffinden einer Vorlage geben sie deren Namen in das Feld **Suche** am oberen Rand des linken Fensters ein. Bereits beim Eintippen werden die Suchergebnisse angezeigt. Zum Löschen des **Suche**-Felds klicken Sie auf **Löschen** rechts davon.

Vorlagen sind in zwei Kategorien unterteilt:

- **Voreinstellungen.** Dies sind vordefinierte, in GravityZone standardmäßig enthaltene Vorlagen.
- **Benutzerdefinierte Vorlagen.** Solche Vorlagen können Sie Ihren Bedürfnissen entsprechend erstellen.

Voreinstellungen

GravityZone enthält fünf Voreinstellungen:

- **Malware-Aktivität**, liefert Ihnen Informationen zu Malware-Bedrohungen, die über einen festgelegten Zeitraum hinweg auf ausgewählten Computern gefunden wurden.

Der Bericht enthält den Namen und die IP der entsprechenden Maschine, den Infektionsstatus (infiziert oder bereinigt), den Namen der Malware, die gegen die Bedrohung ergriffene Maßnahme (ignoriert, vorhanden, gelöscht, blockiert, in Quarantäne, bereinigt oder wiederhergestellt), den Dateityp, den Dateipfad und den gerade eingeloggt Benutzer.

- **Update-Status**, zeigt den Update-Status des auf ausgewählten Zielen installierten Sicherheitsagenten an. Der Bericht enthält den Namen und die IP der entsprechenden Maschine, den Produkt-Update-Status (aktualisiert, veraltet, deaktiviert), den Signature-Update-Status (aktualisiert, veraltet, deaktiviert), den Typ den Sicherheitsagenten, die Produkt- und Signaturversion.
- **Malware-Status** hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Endpunkte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde.

Der Bericht enthält den Namen und die IP der entsprechenden Maschine, den Infektionsstatus (infiziert oder bereinigt), den Namen der Malware, die ergriffene Maßnahme (ignoriert, vorhanden, gelöscht, blockiert, in Quarantäne, bereinigt oder wiederhergestellt).

- **Blockierte Websites** informiert Sie über die Aktivität des Moduls Internet-Zugangssteuerung des Sicherheitsagenten.

Der Bericht enthält den Namen und die IP der entsprechenden Maschine, die Art der Bedrohung (Phishing, Betrug oder nicht vertrauenswürdig), den Namen der Regel, die Website-Kategorie und die blockierte URL.



- **Blockierte Anwendungen**, hilft Ihnen herauszufinden, welche Anwendungen in einem bestimmten Zeitraum blockiert wurden.

Der Bericht liefert Informationen über den Namen und die IP der entsprechenden Maschine, den Namen der blockierten Anwendung, den Dateipfad und die Behandlung der Bedrohung: mit ATC, IDS oder Anwendungssteuerung.



Benutzerdefinierte Vorlagen

Falls Sie eine andere Vorlage benötigen als die in den Voreinstellungen von GravityZone vorhandenen, können Sie Ihre eigene Abfragevorlage erstellen. Sie können beliebig viele Vorlagen speichern.

So erstellen Sie eine benutzerdefinierte Vorlage:


1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie auf die Schaltfläche  **Vorlagen** am oberen Rand der Tabelle. Das Fenster **Vorlagen-Manager**-Konfiguration wird angezeigt.
3. Klicken Sie in der oberen linken Bildschirmcke auf den Button  **Hinzufügen**. Das Abfrage-Formular wird im rechten Fenster angezeigt.
4. Geben Sie die erforderlichen Informationen in das Abfrage-Formular ein. Hinweise zum Ausfüllen des Abfrage-Formulars finden Sie unter [„Abfragen erstellen“ \(S. 476\)](#).
5. Klicken Sie auf **Speichern**. Die neu erstellte Vorlage wird im linken Fenster unter **Benutzerdefinierte Vorlagen** angezeigt.

Sie können auch aus einer voreingestellten Vorlage eine benutzerdefinierte Vorlage erstellen.

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie auf die Schaltfläche  **Vorlagen** am oberen Rand der Tabelle. Das Fenster **Vorlagen-Manager**-Konfiguration wird angezeigt.
3. Wählen Sie im linken Fenster eine Voreinstellung aus. Die entsprechenden Einstellungen werden im rechten Fenster angezeigt.
4. Klicken Sie  **Klonen** in der oberen linken Bildschirmcke an, um eine Kopie der Voreinstellung zu machen.
5. Bearbeiten Sie alle Einstellungen, die Sie für Ihr Abfrage-Formular benötigen. Hinweise zum Ausfüllen des Abfrage-Formulars finden Sie unter [„Abfragen erstellen“ \(S. 476\)](#).
6. Klicken Sie auf **Speichern**. Die neu erstellte Vorlage wird im linken Fenster unter **Benutzerdefinierte Vorlagen** angezeigt.

Wenn Sie eine neue Abfrage erstellen, können Sie diese auch als Vorlage speichern. Weitere Informationen finden Sie unter [„Abfragen erstellen“ \(S. 476\)](#).

Benutzerdefinierte Vorlagen löschen:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie auf die Schaltfläche  **Vorlagen** am oberen Rand der Tabelle. Das Fenster **Vorlagen-Manager**-Konfiguration wird angezeigt.

3. Klicken Sie im Bereich **Benutzerdefinierte Vorlagen** die zu löschende Vorlage an. Die Vorlage-Einstellungen wird im rechten Fenster angezeigt.
4. Klicken Sie **Vorlage löschen** unten im Fenster an und bestätigen Sie dann Ihre Aktion, indem Sie **Ja** anklicken.

Abfragen erstellen

So generieren Sie eine neue Abfrage:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie auf die Schaltfläche **+Hinzufügen** im obeneren Bereich der Tabelle. Ein Konfigurationsfenster wird geöffnet.
3. Um eine voreingestellte oder zuvor generierte Vorlage zu verwenden, klicken Sie das Kästchen **Vorlage verwenden** an.
4. Unter **Details** tragen Sie einen aussagekräftigen Namen für Ihre Abfrage ein. Berücksichtigen Sie bei der Auswahl des Namens den Abfragetyp, das Ziel und andere Einstellungen.
5. Wählen Sie den Abfragetyp aus. Weitere Informationen finden Sie unter [„Abfragetypen“ \(S. 470\)](#)
6. Mit der Schaltfläche **Per E-Mail senden an** senden Sie die Abfrage an bestimmte Empfänger. Geben Sie in das entsprechende Feld so viele E-Mail-Adressen wie gewünscht ein.
7. Im Bereich **Wiederholung** wählen Sie:
 - a. **Datum festlegen** für einen bestimmten Tag.
 - b. **Zeitraum** für ein längeres Zeitintervall.
 - c. Klicken Sie das Kästchen **Wiederholung** an, wenn die Abfrage in bestimmten Intervallen durchgeführt werden soll, die Sie im Bereich **Berichtszeitraum** festlegen können.
8. Konfigurieren Sie die Chart-Einstellungen.
 - a. Wählen Sie aus dem Menü **Typ** ein Diagramm aus, mit dem Sie Ihre Abfrage illustrieren wollen oder wählen Sie **Keine**, wenn Sie keins wünschen. Je nach Abfragetyp und Berichtszeitraum können Sie ein Torten-, Balken- oder Liniendiagramm verwenden.

- b. Im Feld **Wert entnehmen aus** wählen Sie die Datenkategorien, die Sie für Ihre Abfrage benötigen. Jeder Abfragetyp liefert spezifische Informationen zu Endpunkten, Sicherheitsagenten und Sicherheitsereignissen. Weitere Details zu den Typen finden Sie unter „**Abfragetypen**“ (S. 470)
9. Unter **Tabelleneinstellungen** wählen Sie die Spalten aus, die Ihr Bericht enthalten soll. Die hierfür verfügbaren Daten hängen vom ausgewählten Abfragetyp ab und können sich auf Endpunkttyp und OS, Sicherheitsagenten-Status und Vorfälle, Module, Richtlinien und Sicherheitsereignisse beziehen. Alle gewählten Spalten werden in der Tabelle **Spalten** angezeigt. Mit der Drag-and-Drop-Funktion ändern Sie die Reihenfolge.

**Beachten Sie**


Beachten Sie bitte beim Tabellenlayout den verfügbaren Platz. Für eine gute Darstellung im PDF-Dokument sollte Ihre Tabelle maximal 10 Spalten enthalten.

10. Unter **Filter** können Sie das von Ihnen gewünschte Datenset für Ihren Bericht auswählen; verwenden sie dazu die verfügbaren Filterkriterien:
 - a. Wählen Sie im **Filtertyp**-Menü einen Filter aus und klicken Sie dann **+ Filter hinzufügen** an.
 - b. Klicken Sie in der darunter befindlichen Tabelle **Wert** an, um eine oder mehrere Filteroptionen zu festzulegen.

Der **Host OS**-Filter z.B erfordert die Festlegung eines OS-Namens, z.B. Windows oder Linux, während Sie über den Filter **Gerätesteuerungsmodul** aus einer Dropdown-Liste die Endpunkte auswählen können, auf denen das Modul deaktiviert ist.
 - c. Klicken Sie **- Löschen**, um einen Filter zu entfernen.
11. **Ziele wählen**. Scrollen Sie zum Konfigurieren der Berichtsziele nach unten. Wählen Sie eine oder mehrere Gruppen von Endpunkten, die Sie in den Bericht einbeziehen möchten. Über die Ansichtenauswahl können Sie überprüfen, ob Sie in allen Netzwerkansichten die richtigen Ziele markiert haben.
12. Über das Kästchen **Als Vorlage sichern** können Sie diese Einstellungen für weitere Abfragen sichern. Geben Sie dieser Vorlage einen aussagekräftigen Namen.
13. Klicken Sie auf **Generieren**, um die Abfrage anzulegen. Sobald die Abfrage gespeichert ist, erhalten Sie eine Bestätigung im Bereich **Benachrichtigungen**.

Abfragen löschen

So löschen Sie eine Abfrage:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie den Button  **Löschen** am oberen Rand der Tabelle.



Beachten Sie

Beim Löschen einer Abfrage werden auch alle generierten Berichte gelöscht.

9.8.3. Berichte anzeigen und verwalten

Alle abfragebasierten Berichte werden auf der Seite **Berichte > Abfragen** angezeigt.




Beachten Sie

Berichte stehen nur den Benutzern zur Verfügung, die diese auch erstellt haben.

Berichte betrachten

Zur Ansicht eines abfragebasierten Berichts:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Zum leichteren Auffinden von Berichten können Sie diese nach Namen, Typ, Erstellungsdatum oder Berichtszeitraum sortieren. Standardmäßig sind Berichte nach dem aktuellen Erstellungsdatum sortiert.
3. Klicken Sie auf einen beliebigen Namen, um Abfrageinformationen in einem neuen Fenster anzuzeigen. Diese Angaben können nicht bearbeitet werden.
4. Klicken Sie auf das Plus-Zeichen vor dem Namen der Abfrage, um eine Liste mit Berichtsinstanzen anzuzeigen, und auf das Minus-Zeichen, um sie wieder zu schließen.
5. Zur Anzeige der letzten Berichtsinstanz klicken Sie das Feld  **Bericht anzeigen**. Ältere Instanzen sind nur im PDF- oder CSV-Format verfügbar.

Alle Berichte enthalten eine Zusammenfassung im oberen Bereich der Berichtseite und Details auf der unteren Hälfte der Seite.

Die Zusammenfassung enthält Statistikdaten (Torten-, Balken- oder Liniendiagramme) für alle Ziel-Endpunkte und allgemeine Informationen zur Abfrage, z.B. Wiederholungen, Berichtszeitraum, Abfragetyp sowie verwendete Filter.

Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden. Um Daten in der Tabelle anzuzeigen, können Sie auch auf den entsprechenden Bereich in der Grafik klicken.

Der Detailbereich gibt Ihnen Informationen zu jedem Ziel-Endpunkt. Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Um die Spaltenansicht in der Tabelle anzupassen, klicken Sie auf **||| Spalten**.

Berichte speichern

Standardmäßig werden alle Berichte automatisch in Control Center gespeichert. Sie können Berichte auch im PDF- oder CSV-Format auf Ihrem Computer speichern.



So speichern Sie den Bericht auf Ihrem Computer:

- Von der Berichtsseite.
- Aus der **Abfragen**-Tabelle.

Speichern eines Reports, während Sie auf der entsprechenden Seite sind:

1. Klicken Sie auf die Schaltfläche  **Export** in der linken unteren Ecke.
2. Wählen Sie das gewünschte Format für den Bericht:
 - a. Portables Dokumentenformat (PDF) oder
 - b. Comma-Separated-Values (CSV)
3. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.


Exportieren eines Berichts, während Sie auf der Seite **Bericht > Abfragen** sind:

1. Öffnen Sie die Seite **Berichte > Abfragen**.
2. Klicken Sie die Schaltfläche  **PDF** oder  **CSV** für den jeweiligen Bericht.
3. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

Bei allen im PDF-Format exportierten Berichten befinden sich Zusammenfassung und Details im gleichen Dokument auf getrennten A4- oder Querformat-Darstellungen. Der Detailabschnitt ist auf 100 Zeilen pro PDF-Dokument begrenzt.

Berichte per E-Mail versenden

Sie haben zwei Möglichkeiten, Berichte per E-Mail zu senden:

1. Klicken Sie auf der Seite des Berichts, den Sie gerade anzeigen, auf die Schaltfläche  **E-Mail** in der unteren linken Ecke. Der Bericht wird an die mit Ihrem Konto verknüpfte E-Mail-Adresse gesendet.
2. Beim Generieren einer neuen Abfrage klicken Sie das Kästchen **Per E-Mail versenden an** an, und geben Sie die gewünschten E-Mail-Adressen in das entsprechende Feld ein.

Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen. Um einen abfragebasierten Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

10. QUARANTÄNE

Die Quarantäne ist ein verschlüsselter Ordner, in dem potenziell bösartige Dateien aufbewahrt werden, so zum Beispiel vermutlich oder tatsächlich mit Malware infizierte Dateien und andere unerwünschte Dateien. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden, Viren oder andere Malware können also keinen Schaden mehr anrichten.

GravityZone verschiebt Dateien gemäß den Richtlinien, die Endpunkten zugewiesen wurden, in die Quarantäne. Standardmäßig werden Dateien, die nicht desinfiziert werden können, in die Quarantäne verschoben.

Die Quarantäne wird auf jedem lokalen Endpunkt gespeichert, außer beim mit vShield Endpoint und NSX integrierten VMware vCenter-Server, bei dem die Speicherung auf dem Security Server erfolgt.



Wichtig

Für Mobilgeräte steht die Quarantäne nicht zur Verfügung.

10.1. Die Quarantäne im Detail

Auf der **Quarantäne**-Seite finden sich detaillierte Informationen zu allen Dateien, die von allen Endpunkten, die Sie verwalten, in die Quarantäne verschoben wurden.

Vorfälle	Computer	IP	Datei	Name der Bedrohung	Hinzugefügt am	Aktionsstatus
Blockerliste						
Suchen						
Netzwerk	<input type="checkbox"/>	MMH-DOC1	10.0.2.15	C:\Documents and Settings\adm... EICAR-Test-File (not a virus)	12 Mär 2015, 02:59:25	Keine
Pakete	<input type="checkbox"/>	MMH-DOC1	10.0.2.15	C:\Documents and Settings\adm... EICAR-Test-File (not a virus)	12 Mär 2015, 02:27:23	Keine
Aufgaben	<input type="checkbox"/>	MMH-DOC1	10.0.2.15	C:\Documents and Settings\adm... EICAR-Test-File (not a virus)	12 Mär 2015, 02:27:08	Keine
	<input type="checkbox"/>	MMH-DOC1	10.0.2.15	C:\Documents and Settings\adm... EICAR-Test-File (not a virus)	12 Mär 2015, 02:59:33	Keine
Richtlinien						
Zuweisungsregeln						
Berichte						
Quarantäne						
Unternehmen						
Konten						
Benutzeraktivität						

Erste Seite | Seite 1 von 1 | Letzte Seite | 20 | 4 Objekte

Die Quarantäneübersicht

Die Quarantäne-Seite hat zwei Ansichten:


- **Computer und virtuelle Maschinen**, für Dateien, die direkt im Dateisystem der Endpunkte gefunden wurden.
- **Exchange-Server**, für E-Mails und Anhangsdateien, die auf den Exchange-Mail-Servern gefunden wurden.

Mit der Ansichtsauswahl am oberen Rand der Seite können Sie zwischen den beiden Ansichten hin und her wechseln.

Informationen über Dateien in Quarantäne werden in einer Tabelle angezeigt. Je nach Anzahl der verwalteten Endpunkte und dem Ausmaß vergangener Infektionen kann die Quarantäne-Tabelle unter Umständen sehr viele Einträge enthalten. Die Tabelle kann über mehrere Seiten gehen (pro Seite werden standardmäßig nur 20 Einträge angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Um leichter an die gewünschten Informationen zu gelangen, können Sie Suchbegriffe in die Suchfelder der Spaltenüberschriften eingeben. Sie können beispielsweise nach einer bestimmten Bedrohung suchen, die im Netzwerk gefunden wurde, oder nach einem bestimmten Netzwerkobjekt. Sie können auch auf die Spaltenüberschriften klicken, um Daten nach einer bestimmten Spalte zu ordnen.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf  **Neu laden**. Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

10.2. Quarantäne für Computer und virtuelle Maschinen

Dateien in der Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen. Zudem werden die Dateien in Quarantäne nach jedem Update der Malware-Signaturen gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt. Diese Funktionen beziehen sich auf die einzelnen Sicherheitsrichtlinien auf der Seite **Richtlinien**, und Sie können sie entweder beibehalten oder deaktivieren. Weitere Informationen finden Sie unter „Quarantäne“ (S. 298).

10.2.1. Quarantäne-Details anzeigen

Die Quarantäne-Tabelle enthält die folgenden Informationen:

- Der Name des Endpunktes, auf dem die Bedrohung gefunden wurde.
- IP-Adresse des Endpunktes, auf dem die Bedrohung gefunden wurde.
- Pfad zu der infizierten oder verdächtigen Datei auf dem Endpunkt, auf dem sie gefunden wurde.
- Der Name, den die Bitdefender-Sicherheitsexperten der Malware-Bedrohung gegeben haben.
- Zeitpunkt, zu dem die Datei in die Quarantäne verschoben wurde.
- Der Status der Aktion, die auf die in die quarantäneverschobene Datei angewendet werden sollte.

10.2.2. Verwalten von Dateien in der Quarantäne

Die Quarantäne verhält sich je nach Umgebung etwas unterschiedlich:

- **Security for Endpoints** speichert die in die Quarantäne verschobenen Dateien auf jedem verwalteten Computer. Über das Control Center können Sie einzelne Dateien in der Quarantäne löschen oder wiederherstellen.
- **Security for Virtualized Environments (Multi-Plattform)** speichert die in die Quarantäne verschobenen Dateien auf jeder verwalteten virtuellen Maschine. Über das Control Center können Sie einzelne Dateien in der Quarantäne löschen oder wiederherstellen.
- **Security for Virtualized Environments (mit VMware vShield Endpoint oder NSX)** speichert Dateien in Quarantäne in der Security Server-Appliance. Über das Control Center können Sie Dateien in der Quarantäne löschen oder an einen Ort Ihrer Wahl herunterladen.

Dateien aus der Quarantäne wiederherstellen


Es kann vorkommen, dass Sie Dateien in Quarantäne an ihrem Ursprungsort oder an anderer Stelle wiederherstellen müssen. So zum Beispiel, wenn Sie wichtige Dateien wiederherstellen möchten, die einem infizierten Archiv gespeichert sind, das in Quarantäne verschoben wurde.



Beachten Sie

Die Wiederherstellung von Dateien aus der Quarantäne ist nur in Umgebungen möglich, die durch Security for Endpoints und Security for Virtualized Environments (Multi-Plattform) geschützt sind.

Um eine oder mehrere Dateien in Quarantäne wiederherzustellen:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie in der Ansichtsauswahl am oberen Rand der Seite **Computer und Virtuelle Maschinen**.
3. Markieren Sie die Kästchen für die Dateien in Quarantäne, die Sie wiederherstellen möchten.
4. Klicken Sie auf die Schaltfläche  **Wiederherstellen** am oberen Rand der Tabelle.
5. Wählen Sie den Speicherort aus, an dem Sie die ausgewählten Dateien wiederherstellen möchten (entweder der ursprüngliche Speicherort oder ein benutzerdefinierter Speicherort auf dem Ziel-Computer).

Wenn die Wiederherstellung an einem benutzerdefinierten Speicherort stattfinden soll, müssen Sie den absoluten Pfad in das entsprechende Feld eingeben.

6. Wählen Sie **Ausschluss automatisch zur Richtlinie hinzufügen**, um die wiederherzustellenden Dateien von zukünftigen Scans auszuschließen. Der Ausschluss gilt für alle Richtlinien, die sich auf die gewählten Dateien beziehen, außer auf die Standardrichtlinie - diese kann nicht verändert werden.
7. Klicken Sie auf **Speichern**, um die Aktion zum Wiederherstellen einer Datei anzufordern. Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.
8. Die angeforderte Aktion wird sofort an die Ziel-Endpunkte geschickt bzw. sobald diese wieder online sind.

Auf der Seite **Aufgaben** werden Details zum Status der Aktion angezeigt. Sobald eine Datei wiederhergestellt ist, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

Quarantäne-Dateien herunterladen

In VMware-Umgebungen mit vShield Endpoint oder NSX wird die Quarantäne auf dem Security Server gespeichert. Wenn Sie Daten aus Dateien in der Quarantäne einsehen oder wiederherstellen möchten, müssen Sie sie über das Control Center vom Security Server herunterladen. Dateien in der Quarantäne werden als verschlüsseltes, passwortgeschütztes ZIP-Archiv heruntergeladen, um zu verhindern, dass sie das System infizieren.

Um das Archiv zu öffnen und den Inhalt zu extrahieren, müssen Sie das Quarantäne-Tool verwenden. Dabei handelt es sich um eine eigenständige Bitdefender-Anwendung, die nicht installiert werden muss.

Das Quarantäne-Tool steht für die folgenden Betriebssysteme zur Verfügung:

- Windows 7 oder höher
- Die meisten 32-Bit-Linux-Distributionen mit grafischer Benutzeroberfläche.



Beachten Sie

Beachten Sie, dass das Quarantäne-Tool keine Befehlszeilenoberfläche hat.




Warnung

Bei der Extraktion von Quarantäne-Dateien sollten Sie vorsichtig sein, denn sie könnten Ihr System infizieren. Wir empfehlen, die Quarantäne-Dateien auf einem Textsystem oder einem isolierten System zu extrahieren und zu analysieren; vorzugsweise auf einem Linux-System. Malware-Infektionen lassen sich unter Linux leichter eindämmen.

So laden Sie Dateien aus der Quarantäne auf Ihren Computer herunter:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie in der Ansichtsauswahl am oberen Rand der Seite **Computer und Virtuelle Maschinen**.
3. Filtern Sie die Tabellendaten, indem Sie den Hostnamen oder die IP-Adresse des Security Server in das entsprechende Feld der Tabellenüberschrift eingeben.

Wenn viele Dateien in der Quarantäne sind, können Sie zusätzliche Filter anwenden oder mehr Einträge pro Seite anzeigen lassen, um einen leichteren Überblick über die gewünschten Dateien zu bekommen.

4. Markieren Sie die Kästchen der Dateien, die Sie herunterladen möchten.
5. Klicken Sie auf die Schaltfläche  **Herunterladen** am oberen Rand der Tabelle. Je nach Ihren Browser-Einstellungen werden Sie aufgefordert, die Dateien in einem Ordner Ihrer Wahl zu speichern; wenn nicht, werden die Dateien automatisch in den Standard-Download-Ordner heruntergeladen.

So können Sie auf wiederhergestellte Dateien zugreifen:

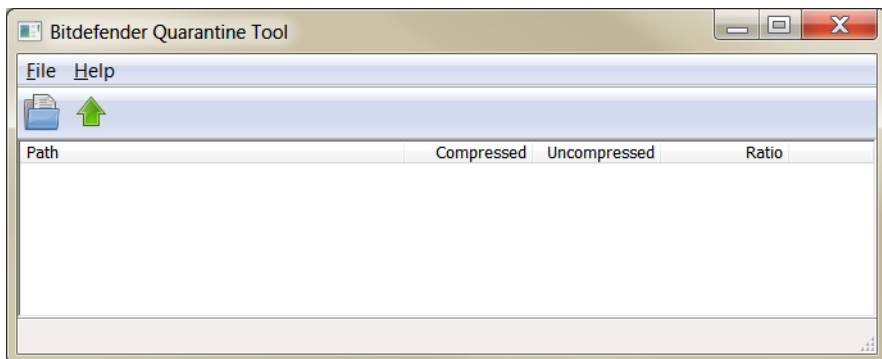
1. Das zu Ihrem Betriebssystem passende Quarantäne-Tool können Sie auf der Seite **Hilfe & Support** oder von einer der folgenden Adressen herunterladen:
 - [Quarantäne-Tool für Windows](#)
 - [Quarantäne-Tool für Linux](#)




Beachten Sie

Das Quarantäne-Tool für Linux ist in einer `tar`-Datei archiviert.


2. Starten Sie die ausführbare Datei des Quarantäne-Tools.



Quarantäne-Tool

- Um das Archiv in das Tool zu laden, können Sie im Menü **Datei** auf **Öffnen** klicken, den Tastaturbefehl Strg+O verwenden oder auf die Schaltfläche  **Öffnen** klicken.

Die Dateien werden im Archiv nach der virtuellen Maschine sortiert, auf der sie gefunden wurden; sie behalten dabei ihren ursprünglichen Pfad.

- Wenn Zugriff-Malware-Scans im System aktiviert sind, sollten Sie sie vor dem Extrahieren der archivierten Dateien deaktivieren oder einen Scan-Ausschluss für den Speicherort einrichten, an den Sie die Dateien extrahieren möchten. Andernfalls wird Ihr Malware-Schutz-Programm die extrahierten Dateien als gefährlich erkennen und entsprechende Aktionen ausführen.
- Wählen Sie die Dateien aus, die Sie extrahieren möchten
- Klicken Sie im Menü **Datei** auf **Extrahieren**, verwenden Sie den Tastaturbefehl Strg+E oder klicken Sie auf die Schaltfläche  **Extrahieren**.
- Wählen Sie den Zielordner. Die Dateien werden an den ausgewählten Speicherort extrahiert, wobei die ursprüngliche Ordnerstruktur beibehalten wird.

Dateien in der Quarantäne automatisch löschen

Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Sie können diese Einstellung ändern, indem Sie die den verwalteten Endpunkten zugewiesene Richtlinie bearbeiten.

Um das Intervall für die automatische Löschung von Dateien in Quarantäne zu ändern:

- Gehen Sie zur **Richtlinien**-Seite.

2. Identifizieren Sie die Richtlinie, die den Endpunkten zugewiesen wurde, auf denen Sie die Einstellung ändern möchten, und klicken Sie auf ihren Namen.
3. Gehen Sie zur Seite **Malware-Schutz > Einstellungen**.
4. Wählen Sie im Bereich **Quarantäne** die Anzahl an Tagen, nach denen Dateien in der Quarantäne gelöscht werden sollen.
5. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Dateien in der Quarantäne manuell löschen

Wenn Sie Dateien in der Quarantäne von Hand löschen möchten, sollten Sie zunächst sicherstellen, dass die von Ihnen ausgewählten Dateien nicht mehr gebraucht werden.

Eine Datei kann unter Umständen auch selbst die Malware sein. Sollten Ihre Nachforschungen dies ergeben, können Sie die Quarantäne nach dieser speziellen Bedrohung durchsuchen und sie aus der Quarantäne löschen.

Um eine oder mehrere Dateien in Quarantäne zu löschen:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie in der Ansichtsauswahl am oberen Rand der Seite **Computer und Virtuelle Maschinen**.
3. Markieren Sie die Kästchen für die Dateien in der Quarantäne, die Sie löschen möchten.
4. Klicken Sie auf die Schaltfläche **☹ Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.

Die angeforderte Aktion wird sofort (bzw. sobald diese wieder online sind) an die entsprechenden Netzwerkobjekte geschickt. Sobald eine Datei gelöscht wurde, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

Leeren der Quarantäne

So löschen Sie alle Objekte in der Quarantäne:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Computer und virtuelle Maschinen** aus der Ansichtsauswahl.
3. Klicken Sie auf **Quarantäne leeren**.

Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Alle Einträge in der Quarantäne-Tabelle werden gelöscht. Die angeforderte Aktion wird sofort (bzw. sobald diese wieder online sind) an die entsprechenden Netzwerkobjekte geschickt.

10.3. Exchange-Server-Quarantäne

Die Exchange-Quarantäne enthält E-Mails und Anhänge. Das Malware-Schutz-Modul verschiebt E-Mail-Anhänge in die Quarantäne, der Spam-Schutz sowie die Inhalts- und Anhangsfilterung hingegen verschieben die ganze E-Mail.

Beachten Sie

Die Quarantäne für Exchange-Server benötigt zusätzlichen Festplattenspeicher auf der Partition, auf der der Sicherheitsagent installiert ist. Die Größe der Quarantäne hängt davon ab, wie viele Objekte sich darin befinden und wie groß diese sind.

10.3.1. Quarantäne-Details anzeigen

Die **Quarantäne**-Seite enthält detaillierte Informationen zu in die Quarantäne verschobenen Objekten von allen Exchange-Servern innerhalb Ihres Unternehmens. Die Informationen verteilen Sie auf die Quarantäne-Tabelle und das jeweilige Detailfenster jedes Objekts.

Die Quarantäne-Tabelle enthält die folgenden Informationen:

- **Betreff.** Der Betreff der in die Quarantäne verschobenen E-Mail.
- **Absender.** Die E-Mail-Adresse des Absenders wie sie im Feld **Von** des E-Mail-Headers erscheint.
- **Empfänger.** Die Liste der Empfänger, wie sie in den Feldern **An** und **CC** des E-Mail-Headers erscheinen
- **Tatsächliche Empfänger.** Die Liste der einzelnen Benutzer-E-Mail-Adressen, an die die E-Mail zugestellt werden sollte, bevor sie in die Quarantäne verschoben wurde.
- **Status.** Der Objektstatus nach Abschluss des Scans. Der Status zeigt an, ob eine E-Mail als Spam markiert wurde oder unerwünschte Inhalte hat bzw. ob ein Anhang mit Malware infiziert ist oder unter Verdacht steht, infiziert, unerwünscht oder nicht scanbar zu sein.

- **Name der Malware.** Der Name, den die Bitdefender-Sicherheitsexperten der Malware-Bedrohung gegeben haben.
- **Servername.** Der Hostname des Servers, auf dem die Bedrohung gefunden wurde.
- **Hinzugefügt am.** Zeitpunkt, zu dem die Datei in die Quarantäne verschoben wurde.
- **Aktionsstatus.** Der Status der Aktion, die für das in die Quarantäne verschobene Objekt ausgeführt wurde. So können Sie auf einen Blick sehen, ob eine Aktion evtl. noch aussteht oder fehlgeschlagen ist.



Beachten Sie

- Die Spalten **Tatsächliche Empfänger**, **Name der Malware** und **Servername** sind in der Standardansicht ausgeblendet.
- Wenn mehrere Anhänge derselben E-Mail in die Quarantäne verschoben werden, werden in der Quarantäne-Tabelle separate Einträge für jeden dieser Anhänge gemacht.

So passen Sie die Quarantänedetails an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **III Spalten** auf der rechten Seite der Tabellenüberschrift.
2. Wählen Sie die Spalten, die Sie anzeigen möchten.

Wenn Sie auf die Schaltfläche **Zurücksetzen** klicken, wird wieder die Standardansicht der Spalten angezeigt.

Wenn Sie auf den **Betreff**-Link eines Objektes klicken, erhalten Sie weitere Informationen. Es wird dann das Fenster **Objektdetails** angezeigt, das die folgenden Informationen enthält:

- **In die Quarantäne verschobenes Objekt.** Typ des Objektes in Quarantäne, entweder E-Mail oder Anhang.
- **Hinzugefügt am.** Zeitpunkt, zu dem die Datei in die Quarantäne verschoben wurde.
- **Status.** Der Objektstatus nach Abschluss des Scans. Der Status zeigt an, ob eine E-Mail als Spam markiert wurde oder unerwünschte Inhalte hat bzw. ob ein Anhang mit Malware infiziert ist oder unter Verdacht steht, infiziert, unerwünscht oder nicht scanbar zu sein.

- **Name des Anhangs.** Der Name der angehängten Datei, die vom Malware-Schutz- oder vom Anhangsfilterungsmodul gefunden wurde.
- **Name der Malware.** Der Name, den die Bitdefender-Sicherheitsexperten der Malware-Bedrohung gegeben haben. Diese Information steht nur zur Verfügung, wenn das Objekt infiziert war.
- **Scan-Ort.** Ein Objekt wird entweder auf der Transportebene gefunden oder in einem Postfach oder öffentlichen Ordner des Exchange-Speichers.
- **Übereinstimmende Regel.** Die Richtlinienregel, die mit der Bedrohung übereinstimmt.
- **Server.** Der Hostname des Servers, auf dem die Bedrohung gefunden wurde.
- **IP-Adresse des Absenders.** Die IP-Adresse des Absenders.
- **Absender (von).** Die E-Mail-Adresse des Absenders, wie sie im Feld **Von** des E-Mail-Headers erscheint.
- **Empfänger.** Die Liste der Empfänger, wie sie in den Feldern **An** und **CC** des E-Mail-Headers erscheinen
- **Tatsächliche Empfänger.** Die Liste der einzelnen Benutzer-E-Mail-Adressen, an die die E-Mail zugestellt werden sollte, bevor sie in die Quarantäne verschoben wurde.
- **Betreff.** Der Betreff der in die Quarantäne verschobenen E-Mail.



Beachten Sie

Die Auslassungspunkte am Ende eines Textes weisen darauf hin, dass ein Teil des Textes nicht angezeigt wird. In solchen Fällen können Sie mit der Maus über den Text fahren, um den gesamten Text in einem Tooltip anzuzeigen.

10.3.2. In die Quarantäne verschobene Objekte

Durch das Exchange-Schutz-Modul in Quarantäne gestellte Emails und Dateien werden auf dem lokalen Server als verschlüsselte Dateien gespeichert. Über Control-Center haben Sie die Möglichkeit, in Quarantäne befindliche E-Mails wiederherzustellen oder in Quarantäne befindliche E-Mails bzw. Dateien zu löschen oder zu speichern.


In Quarantäne befindliche E-Mails wiederherstellen

Wenn Sie sich sicher sind, dass eine E-Mail, die in die Quarantäne verschoben wurde, keine tatsächliche Bedrohung darstellt, können Sie sie wieder aus der Quarantäne heraus holen. Über Exchange-Web-Services sendet Exchange-Schutz die in Quarantäne befindliche E-Mail als Anhang einer Bitdefender-Benachrichtigungs-E-Mail an den vorgesehenen Empfänger.

Beachten Sie

Es können nur E-Mails wiederhergestellt werden. Um einen Anhang wiederherzustellen, müssen Sie ihn in einem lokalen Ordner auf dem Exchange-Server speichern.

So stellen Sie eine oder mehrere E-Mails wieder her:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Exchange** aus der Ansichtsauswahl am oberen Rand der Seite.
3. Markieren Sie die Kästchen für die E-Mails, die Sie wiederherstellen möchten.
4. Klicken Sie auf die Schaltfläche  **Wiederherstellen** am oberen Rand der Tabelle. Das Fenster **Zugangsdaten wiederherstellen** wird angezeigt.
5. Wählen Sie die Zugangsdaten eines Exchange-Benutzers ein, der berechtigt ist, die wiederherzustellenden E-Mails zu versenden. Wenn die Zugangsdaten, die Sie verwenden möchten, noch neu sind, müssen Sie sie zunächst dem Zugangsdaten-Manager hinzufügen.


So fügen Sie die benötigten Zugangsdaten hinzu:

- a. Geben Sie die erforderlichen Informationen in die entsprechenden in der Tabellenüberschrift gekennzeichneten Felder ein:
 - Den Benutzernamen und das Passwort des Exchange-Benutzers.

Beachten Sie

Der Benutzername muss den Domain-Namen enthalten, z. B. Benutzer@Domain oder Domain\Benutzer.


- Die E-Mail-Adresse des Exchange-Benutzers, diese muss nur eingegeben werden, wenn die E-Mail-Adresse von Benutzernamen abweicht.
- Die URL für Exchange Web Services (EWS), diese muss nur eingegeben werden, wenn die Exchange-AutoErmittlung nicht funktioniert. Dies ist normalerweise bei Edge-Transport-Servern in einer DMZ der Fall.

- b. Klicken Sie auf die Schaltfläche  **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.
6. Klicken Sie auf **Wiederherstellen**. Eine Bestätigungsmeldung wird angezeigt. Die entsprechende Aktion wird sofort an die Server gesendet. Sobald eine Email wiederhergestellt ist, wird sie aus der Quarantäne entfernt; der entsprechende Eintrag in der Quarantäne-Tabelle wird gelöscht.
Der Wiederherstellungs-Status kann an den folgenden Stellen überprüft werden:
 - Spalte **Aktionsstatus** in der Quarantäne-Tabelle.
 - **Netzwerk > Aufgaben** -Seite.

Dateien aus der Quarantäne speichern

Falls Sie Daten untersuchen oder aus den Quarantäne-Dateien entfernen wollen, können diese in einem lokalen Ordner im Exchange-Server gespeichert werden. Bitdefender Endpoint Security Tools entschlüsselt die Dateien und speichert sie an dem festgelegten Ort.

So speichern Sie eine oder mehrere in die Quarantäne verschobene Dateien:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Exchange** aus der Ansichtsauswahl am oberen Rand der Seite.
3. Nutzen Sie Filter, um die Dateien anzuzeigen, die Sie speichern möchten. Geben Sie dazu Suchbegriffe in die Felder der Spaltenüberschriften ein.
4. Markieren Sie die Kästchen für die Dateien in Quarantäne, die Sie wiederherstellen möchten.
5. Klicken Sie auf die Schaltfläche  **Speichern** am oberen Rand der Tabelle.
6. Geben Sie den Pfad zum gewünschten Ordner auf dem Exchange-Server ein. Wenn der Ordner auf dem Server noch nicht existiert, wird er erstellt.



Wichtig

Sie müssen diesen Ordner vom System-Scan ausschließen, da die dort gespeicherten Dateien sonst direkt wieder in die Quarantäne für Computer und virtuelle Maschinen verschoben werden. Weitere Informationen finden Sie unter „Ausschlüsse“ (S. 301).

7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Der Status "Ausstehend" wird in der Spalte **Aktionsstatus** angezeigt. Auf der Seite **Netzwerk > Aufgaben** können Sie auch den Aktionsstatus sehen.

Dateien in der Quarantäne automatisch löschen


Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Sie können diese Einstellung ändern, indem Sie die Richtlinie, die diesem Exchange-Server zugewiesen ist, bearbeiten.

Um das Intervall für die automatische Löschung von Dateien in Quarantäne zu ändern:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie dazu auf den Namen der Richtlinie, die dem gewünschten Exchange-Server zugewiesen ist.
3. Gehen Sie zur Seite **Exchange-Schutz > Allgemein**.
4. Wählen Sie im Bereich **Einstellungen** die Anzahl an Tagen, nach denen Dateien in der Quarantäne gelöscht werden sollen.
5. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Dateien in der Quarantäne manuell löschen

So löschen Sie ein oder mehrere Objekte in der Quarantäne:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Exchange** aus der Ansichtsauswahl.
3. Markieren Sie die Kästchen für die Dateien, die Sie löschen möchten.
4. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Der Status "Ausstehend" wird in der Spalte **Aktionsstatus** angezeigt.

Die entsprechende Aktion wird sofort an die Server gesendet. Sobald eine Datei gelöscht wurde, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

Leeren der Quarantäne

So löschen Sie alle Objekte in der Quarantäne:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Exchange** aus der Ansichtsauswahl.

3. Klicken Sie auf **Quarantäne leeren**.

Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.
Alle Einträge in der Quarantäne-Tabelle werden gelöscht. Die angeforderte Aktion wird sofort an die Ziel-Netzwerkobjekte übermittelt.

11. VERWENDEN DES SANDBOX ANALYZERS

Die Seite **Sandbox Analyzer** bietet eine einheitliche Oberfläche zum Anzeigen, Filtern und Suchen von **automatischen** und **manuellen Übermittlungen** an die Sandbox-Umgebung. Die **Sandbox Analyzer**-Seite umfasst zwei Bereiche:

Die Sandbox Analyzer-Seite

1. Im **Filterbereich** können Sie Eingaben nach verschiedenen Kriterien durchsuchen und filtern: Name, Hash, Datum, Analyseergebnis, Status, Detonationsumgebung und MITREs ATT&CK-Techniken.
2. Im **Bereich der Übermittlungskarten** werden alle Übermittlungen in einem kompakten Format mit detaillierten Informationen zu den einzelnen Übermittlungen angezeigt.

Auf der Seite Sandbox Analyzer haben Sie folgende Möglichkeiten:


- **Übermittlungskarten filtern**
- **Übermittlungsliste und Analysedetails anzeigen**
- **Erneute Übermittlung von Stichproben zur Analyse über die Übermittlungskarte**
- **Übermittlungskarten löschen**
- **Manuelle Übermittlung vornehmen.**

11.1. Filtern von Übermittlungskarten

Im Filterbereich können Sie Folgendes tun:

- Übermittlungen nach verschiedenen Kriterien filtern. Die Seite lädt automatisch nur die Karten der Sicherheitsereignisse, die zu den ausgewählten Filterkriterien passen.
- Filter zurücksetzen, indem Sie auf **Filter löschen** klicken.
- Den Filterbereich ausblenden, indem Sie auf **Filter ausblenden** klicken. Sie können die ausgeblendeten Optionen wieder anzeigen, indem Sie auf **Filter anzeigen** klicken.

Sie können die Sandbox Analyzer-Übermittlungen nach den folgenden Kriterien filtern:

- **Name der Stichprobe und Hash (MD5)**. Geben Sie in das Suchfeld einen Teil oder den gesamten Namen oder den Hash der gesuchten Stichprobe ein und klicken Sie rechts auf die Schaltfläche **Suchen**.
- **Datum**. Gehen Sie folgendermaßen vor, um nach dem Datum zu filtern:
 1. Klicken Sie auf das Kalendersymbol , um den Suchzeitraum zu festzulegen.
 2. Legen Sie den Zeitraum fest. Klicken Sie oben auf die Schaltflächen **Von** und **Bis**, um Start- und Enddatum des Zeitraums festzulegen. Aus der Liste rechts können Sie auch einen vordefinierten Zeitraum (relativ zum aktuellen Datum) auswählen, z. B. Letzte 30 Tage.
Unterhalb des Kalenders können Sie die Zeitpunkte auf Stunde und Minute genau festlegen.
 3. Klicken Sie auf **OK** um den Filter anzuwenden.
- **Analyseergebnis**. Wählen Sie eine oder mehrere der folgenden Optionen aus:
 - **Sauber** - von der Stichprobe geht keine Gefahr aus.
 - **Infiziert** - von der Stichprobe geht eine Gefahr aus.
 - **Nicht unterstützt** - die Stichprobe liegt in einem Format vor, das vom Sandbox Analyzer nicht ausgeführt werden kann. Eine vollständige Liste der vom Sandbox Analyzer unterstützten Dateitypen und -erweiterungen finden Sie unter [„Unterstützte Dateitypen und Dateierweiterungen für die manuelle Übermittlung“](#) (S. 549).

- **Schweregradbewertung.** Dieser Wert gibt an, wie gefährlich eine Stichprobe auf einer Skala von 100 bis 0 (Null) ist. Je höher die Zahl, desto gefährlicher ist die Stichprobe. Der Schweregradbewertung erfolgt für alle übermittelten Stichproben, einschließlich derjenigen mit dem Status **Sauber** oder **Nicht unterstützt**.
- **Art der Einreichung.** Wählen Sie eine oder mehrere der folgenden Optionen aus:
 - **Manuell.** Sandbox Analyzer hat die Stichprobe über die Option **Manuelle Übermittlung** erhalten.
 - **Endpunktsensor.** Bitdefender Endpoint Security Tools hat die Stichprobe anhand von Richtlinienereinstellungen an den Sandbox Analyzer übermittelt.
 - **Netzwerkdatenverkehrsensor.** Der Netzwerksensor hat die Stichprobe anhand von Richtlinienereinstellungen an eine lokale Sandbox Analyzer-Instanz übermittelt.
 - **Zentrale Quarantäne.** GravityZone hat die Stichprobe anhand von Richtlinienereinstellungen an eine lokale Sandbox Analyzer-Instanz übermittelt.
 - **API.** Die Stichprobe wurde unter Nutzung von API-Methoden an eine lokale Sandbox Analyzer-Instanz übermittelt.
 - **ICAP-Sensor.** Security Server hat die Stichprobe nach dem Scannen eines ICAP-Servers an eine lokale Sandbox Analyzer-Instanz übermittelt.
- **Übermittlungsstatus.** Markieren Sie eins oder mehrere der folgenden Kästchen:
 - **Fertig** - Sandbox Analyzer hat das Ergebnis der Analyse bereitgestellt.
 - **Analyse ausstehend** - Sandbox Analyzer führt die Stichprobe gerade aus.
 - **Fehlgeschlagen** – Sandbox Analyzer konnte die Stichprobe nicht ausführen.
- **Umgebung.** Hier finden Sie eine Liste der virtuellen Maschinen, die für die Detonation zur Verfügung stehen, einschließlich der von Bitdefender gehosteten Sandbox Analyzer-Instanz. Markieren Sie ein oder mehrere Kästchen, um anzuzeigen, welche Stichproben in bestimmten Umgebungen detoniert wurden.
- **ATT&CK-Techniken.** Mit dieser Filteroption werden, wenn möglich, die Werte aus der MITRE-ATT&CK-Datenbank mit einbezogen. Die Werte der ATT&CK-Techniken ändern sich dynamisch, basierend auf den Sicherheitsereignissen.

Klicken Sie auf den Link **Über** um die ATT&CK-Matrix in einem neuen Reiter zu öffnen.

11.2. Anzeigen von Analysedetails

Auf der Seite **Sandbox Analyzer** werden die Übermittlungskarten nach Tagen in umgekehrter chronologischer Reihenfolge angezeigt. Die Übermittlungskarten enthalten die folgenden Daten:

- Analyseergebnis
- Name der Stichprobe
- Art der Einreichung
- Schweregradbewertung
- Beteiligte Dateien und Prozesse
- Detonationsumgebung
- Hash-Wert (MD5)
- ATT&CK-Techniken
- Status der Einreichung, wenn ein Ergebnis nicht verfügbar ist

Jede Übermittlungskarte enthält, falls vorhanden, einen Link zum detaillierten HTML-Analysebericht. Klicken Sie auf die Schaltfläche **Anzeigen** rechts auf der Karte, um den Bericht zu öffnen.

Der HTML-Bericht enthält umfangreiche, in verschiedenen Ebenen gegliederte Informationen und veranschaulicht anhand von Text, Diagrammen und Bildschirmaufnahmen das Verhalten der Stichprobe in der Detonationsumgebung. Ein Sandbox Analyzer-HTML-Bericht liefert die folgenden Informationen:

- Allgemeine Daten über die analysierte Stichprobe, so z. B.: Name und Klassifizierung der Malware, Übermittlungsdetails (Dateiname, Typ und Größe, Hash, Übermittlungszeitpunkt und Analysedauer).
- Die Ergebnisse der Verhaltensanalyse, die alle während der Detonation erfassten Sicherheitsereignisse beinhalten, unterteilt in Abschnitte. Die Sicherheitsereignisse beziehen sich auf:
 - Schreiben, Löschen, Verschieben, Kopieren, Ersetzen von Dateien im System und auf tragbaren Datenträgern.
 - Ausführen von neu erstellten Dateien.
 - Änderungen am Dateisystem.
 - Änderungen an den laufenden Anwendungen innerhalb einer virtuellen Maschine.
 - Änderungen an der Windows-Taskleiste und am Startmenü.
 - Erstellen, Beenden, Injizieren von Prozessen.
 - Schreiben oder Löschen von Registrierungsschlüsseln.
 - Erstellen von Mutex-Objekten.

- Erstellen, Starten, Anhalten, Modifizieren, Abfragen, Löschen von Diensten.
- Ändern der Browser-Sicherheitseinstellungen.
- Änderung der Windows-Explorer-Anzeigeinstellungen.
- Hinzufügen von Dateien zur Firewall-Ausnahmeliste.
- Änderung von Netzwerkeinstellungen.
- Aktivieren einer Ausführung beim Systemstart.
- Herstellen einer Verbindung zu einem entfernten Host.
- Zugriff auf bestimmte Domains.
- Transfer von Daten von und zu bestimmten Domains.
- Zugriff auf URLs, IP-Adressen und Ports über verschiedene Kommunikationsprotokolle.
- Überprüfen der Indikatoren virtueller Umgebungen.
- Überprüfen der Indikatoren von Überwachungstools.
- Erstellen von Bildschirm- oder Systemabbildern.
- SSDT, IDT, IRP-Hooks.
- Speicherabbilder für verdächtige Prozesse.
- Windows-API-Funktionsaufrufe.
- Wechsel in die Inaktivität für einen bestimmten Zeitraum zur Verzögerung der Ausführung.
- Erstellen von Dateien, die in bestimmten zeitlichen Intervallen auszuführende Aktionen beinhalten.



Wichtig

HTML-Berichte sind nur in Englisch verfügbar, unabhängig von der Sprache, die Sie für GravityZone Control Center festgelegt haben.

11.3. Erneute Übermittlung von Stichproben

Im Bereich der Übermittlungskarten können Sie bereits detonierte Stichproben erneut an eine lokale Sandbox Analyzer-Instanz übermitteln, ohne sie erneut hochladen zu müssen. Diese Möglichkeit besteht für Stichproben, die zuvor mit einem beliebigen Sensor oder einer beliebigen Methode, automatisch, manuell oder über die API an die lokale Sandbox Analyzer-Instanz übermittelt wurden.

Gehen Sie zur erneuten Übermittlung einer Stichprobe wie folgt vor:

1. Klicken Sie in der Übermittlungskarte auf **Erneut zur Analyse übermitteln**.
2. Im Konfigurationsfenster können Sie die Einstellungen der vorherigen Übermittlung beibehalten oder sie wie folgt anpassen:

- a. Wählen Sie unter **Image-Verwaltung** das virtuelle Maschinen-Image aus, das Sie für die Detonation verwenden möchten.
 - b. Nehmen Sie unter **Detonationskonfigurationen** die folgenden Einstellungen vor:
 - i. **Zeitbegrenzung für die Detonation der Stichproben (Minuten)**. Legen Sie einen Zeitraum für den Abschluss der Stichprobenanalyse fest. Der Standardwert beträgt 4 Minuten, in manchen Fällen kann die Analyse aber mehr Zeit in Anspruch nehmen. Nach Ablauf des festgelegten Zeitraums unterbricht der Sandbox Analyzer die Analyse und erstellt einen Bericht auf Grundlage der bis zu diesem Zeitpunkt gesammelten Daten. Wird die Analyse vor Abschluss abgebrochen, liefert sie unter Umständen ungenaue Ergebnisse.
 - ii. **Anzahl der erlaubten Wiederholungen**. Im Falle unerwarteter Fehler versucht der Sandbox Analyzer, eine Stichprobe so oft wie konfiguriert zu detonieren, bis die Analyse abgeschlossen ist. Der Standardwert ist 2. Das bedeutet, dass der Sandbox Analyzer im Fehlerfall noch zweimal versucht, die Stichprobe zu detonieren.
 - iii. **Vorfilterung**. Aktivieren Sie diese Option, um bereits analysierte Proben von der Detonation auszuschließen.
 - iv. **Internetzugang während der Detonation**. Zum Abschluss der Analyse wird für manche Stichproben eine Internetverbindung benötigt. Für ein optimales Ergebnis empfehlen wir, diese Option aktiviert zu lassen.
 - c. Unter **Detonationssprofil** können Sie den Komplexitätsgrad der Verhaltensanalyse festlegen. Dies hat Auswirkungen auf den Durchsatz des Sandbox Analyzers. Wenn Sie beispielsweise **Hoch** auswählen, führt der Sandbox Analyzer im gleichen Zeitraum eine genauere Analyse mit weniger Stichproben durch als bei **Mittel** oder **Gering**.
3. Klicken Sie auf **Erneut übermitteln**.

Nach der erneuten Übermittlung zeigt die Seite **Sandbox Analyzer** eine neue Karte an und die Datenaufbewahrung für diese Stichprobe wird entsprechend verlängert.



Beachten Sie

Die Option **Erneut zur Analyse übermitteln** ist für Stichproben verfügbar, die noch im Sandbox Analyzer-Datenspeicher vorliegen. Stellen Sie sicher, dass die Datenaufbewahrung auf der Seite **Sandbox Analyzer > Sandbox Manager** der Richtlinieneinstellungen konfiguriert ist.

11.4. Löschen von Übermittlungskarten

So löschen Sie nicht mehr benötigte Übermittlungskarten:

1. Rufen Sie die zu löschende Übermittlungskarte auf.
2. Klicken Sie links auf der Karte auf die Option **Eintrag löschen**
3. Zum Bestätigen der Aktion klicken Sie **Ja**.

i Beachten Sie

Auf diese Weise löschen Sie nur die Übermittlungskarte selbst. Alle Informationen zur Übermittlung sind auch weiterhin im Bericht **Sandbox Analyzer-Ergebnisse (veraltet)** verfügbar. Dieser Bericht wird jedoch nur noch eine begrenzte Zeit lang unterstützt.

11.5. Manuelle Übermittlung

Über **Sandbox Analyzer > Manuelle Übermittlung** können Sie Stichproben von verdächtigen Objekten an den Sandbox Analyzer übermitteln, um zu ermitteln, ob es sich dabei um Bedrohungen oder harmlose Dateien handelt. Alternativ können Sie die Seite **Manuelle Übermittlung** auch aufrufen, indem Sie oben rechts im Filterbereich der Seite Sandbox Analyzer auf die Schaltfläche **Stichprobe übermitteln** klicken.

i Beachten Sie

Die manuelle Übermittlung an den Sandbox Analyzer funktioniert mit allen Internet-Browsern, die vom Control Center unterstützt werden, außer Internet Explorer 9. Um Objekte an den Sandbox Analyzer zu übermitteln, melden Sie sich mit einem beliebigen anderen unterstützten Internet-Browser (siehe „[Verbinden mit dem Control Center](#)“ (S. 20)) am Control Center an.

<ul style="list-style-type: none"> Dashboard Netzwerk <ul style="list-style-type: none"> Anwendungsbestand Pakete Aufgaben Richtlinien <ul style="list-style-type: none"> Zuweisungsregeln Berichte Quarantäne Konten <ul style="list-style-type: none"> Benutzeraktivität Systemstatus Sandbox Analyzer <ul style="list-style-type: none"> <li style="color: blue;">Manuelle Übermittlung Infrastruktur Konfiguration <ul style="list-style-type: none"> Update 	<div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 10px;"> Hochladen Allgemeine Einstellungen </div> <h3 style="margin: 0;">Stichproben</h3> <p><input checked="" type="radio"/> Dateien</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right; margin-top: 5px;">Durchsuch</div> <p style="margin-top: 10px;">Geben Sie ein Passwort für die verschlüsselten Archive an:</p> <div style="border: 1px solid #ccc; height: 25px; width: 100%;"></div> <p style="font-size: 0.9em; margin-top: 5px;">Sie können jeweils ein einzelnes Passwort hinzufügen. Wenn Sie mehrere verschlüsselte Archive hochladen, verwendet der Sandbox Analyzer für alle Archive das gleiche Passwort.</p> <p><input type="radio"/> URL</p> <div style="border: 1px solid #ccc; height: 25px; width: 100%;"></div> <h3 style="margin: 10px 0 0 0;">Detonationseinstellungen</h3> <p><input type="checkbox"/> Cloud Sandbox Analyzer verwenden</p> <p>Lokaler Sandbox Analyzer: <input type="text" value="bitdefender-sba-e508 ()"/></p> <p>Image: <input type="text" value="win10_x64_rs6_8n23, win10_x64"/></p> <p>Befehlszeilenargumente: <input type="text"/></p> <p><input checked="" type="checkbox"/> Stichproben einzeln detonieren</p>
--	---

Sandbox Analyzer > Manuelle Übermittlung

So übermitteln Sie Stichproben an den Sandbox Analyzer:

1. Wählen Sie unter **Stichproben** auf der Seite **Hochladen** den Objekttyp aus:
 - a. **Dateien**. Klicken Sie auf die **Durchsuchen**-Schaltfläche, um die Objekte auszuwählen, die Sie zur Verhaltensanalyse übermitteln möchten. Im Falle von passwortgeschützten Archiven können Sie in einem eigenen Feld ein Passwort für die jeweilige Upload-Sitzung festlegen. Während des Analysevorgangs verwendet der Sandbox Analyzer das angegebene Passwort für alle übermittelten Archive.
 - b. **URL**. Geben Sie in das entsprechende Feld eine beliebige URL zur Analyse ein. Sie können nur eine URL pro Sitzung übermitteln.
2. Unter **Detonationseinstellungen** können Sie die Analyseparameter für die aktuelle Sitzung konfigurieren:

- Die Sandbox Analyzer-Instanz, die Sie verwenden möchten. Sie können entweder die Cloud-Instanz oder eine lokal installierte Sandbox Analyzer-Instanz auswählen.
Wenn Sie sich für die Verwendung einer lokalen Sandbox Analyzer-Instanz entscheiden, können Sie mehrere virtuelle Maschinen auswählen, an die Sie die Stichprobe gleichzeitig übermitteln können.
 - **Befehlszeilenargumente.** Sie können beliebig viele Befehlszeilenargumente getrennt durch Leerzeichen hinzufügen, um die Funktionsweise bestimmter Programme, wie beispielsweise ausführbarer Dateien, zu ändern. Die Befehlszeilenargumente gelten während der Analyse für alle übermittelten Stichproben.
 - **Stichproben einzeln detonieren.** Markieren Sie das Kästchen, um die Dateien aus der gebündelten Übermittlung einzeln zu analysieren.
3. Unter **Detonationssprofil** können Sie den Komplexitätsgrad der Verhaltensanalyse festlegen. Dies hat Auswirkungen auf den Durchsatz des Sandbox Analyzers. Wenn Sie beispielsweise **Hoch** auswählen, führt der Sandbox Analyzer im gleichen Zeitraum eine genauere Analyse mit weniger Stichproben durch als bei **Mittel** oder **Gering**.
4. Auf der Seite **Allgemeine Einstellungen** können Sie sitzungsunabhängige Einstellungen vornehmen, die für alle manuellen Übermittlungen gelten:
- a. **Zeitbegrenzung für die Detonation der Stichproben (Minuten).** Legen Sie einen Zeitraum für den Abschluss der Stichprobenanalyse fest. Der Standardwert beträgt 4 Minuten, in manchen Fällen kann die Analyse aber mehr Zeit in Anspruch nehmen. Nach Ablauf des festgelegten Zeitraums unterbricht der Sandbox Analyzer die Analyse und erstellt einen Bericht auf Grundlage der bis zu diesem Zeitpunkt gesammelten Daten. Wird die Analyse vor Abschluss abgebrochen, liefert sie unter Umständen ungenaue Ergebnisse.
 - b. **Anzahl der erlaubten Wiederholungen.** Im Falle unerwarteter Fehler versucht der Sandbox Analyzer, eine Stichprobe so oft wie konfiguriert zu detonieren, bis die Analyse abgeschlossen ist. Der Standardwert ist 2. Das bedeutet, dass der Sandbox Analyzer im Fehlerfall noch zweimal versucht, die Stichprobe zu detonieren.
 - c. **Vorfilterung.** Aktivieren Sie diese Option, um bereits analysierte Proben von der Detonation auszuschließen.

- d. **Internetzugang während der Detonation.** Zum Abschluss der Analyse wird für manche Stichproben eine Internetverbindung benötigt. Für ein optimales Ergebnis empfehlen wir, diese Option aktiviert zu lassen.
- e. Klicken Sie auf **Speichern**, um die Änderungen beizubehalten.
5. Gehen Sie zurück zur Seite **Hochladen**.
6. Klicken Sie auf **Senden**. Ein Fortschrittsbalken zeigt den Status der Übermittlung an.

Nach der Übermittlung wird auf der Seite **Sandbox Analyzer** eine neue Karte angezeigt. Nach Abschluss der Analyse finden Sie auf dieser Karte das Urteil und die entsprechenden Detailinformationen.



Beachten Sie

Zur manuellen Übermittlung an den Sandbox Analyzer müssen Sie über **Netzwerke verwalten**-Rechte verfügen.

11.6. Verwalten der Sandbox Analyzer-Infrastruktur

Im Abschnitt **Sandbox Analyzer > Infrastruktur** stehen die folgenden Aktionen im Zusammenhang mit der lokal installierten Sandbox Analyzer-Instanz zur Auswahl:

- [Status der Sandbox Analyzer-Instanz überprüfen](#)
- [Gleichzeitige Detonationen konfigurieren](#)
- [Status der virtuellen Maschinen-Images überprüfen](#)
- [Virtuelle Maschinen-Images konfigurieren und verwalten](#)

11.6.1. Überprüfen des Sandbox Analyzer-Status

Nach Bereitstellung und Konfiguration der virtuellen Sandbox Analyzer-Appliance auf dem ESXi-Hypervisor können Sie Informationen über die lokale Sandbox Analyzer-Instanz auf der Seite **Status** abrufen.

Dashboard	Status Image-Verwaltung					
Netzwerk	Neu laden					
Anwendungsbestand						
Pakete						
Aufgaben						
Richtlinien						
Zuweisungsregeln						
Berichte						
Quarantäne						
Konten						
Benutzeraktivität						
Systemstatus						
Sandbox Analyzer						
Manuelle Übermittlung						
Infrastruktur						

Sandbox Analyzer-Instanz	Detonierte Stichproben	Datenträgerverw...	Status	Maximale gleichzeitige Detonationen	Konfigurierte gleichzeitige Detonationen
bitdefender-sba-e508	30	65%	Um 15:42 Uhr am 1...	21	0
bitdefender-sba-4h6e	N/A	0%	nicht installiert	21	0
bitdefender-sba-tpf3	N/A	51%	Online	21	2
bitdefender-sba-q0qs	N/A	51%	Online	21	2

Sandbox Analyzer > Infrastruktur > Status

In der Tabelle finden Sie die folgenden Informationen:

- **Name der Sandbox Analyzer-Instanz.** Jeder Name entspricht einer Sandbox Analyzer-Instanz, die auf einem ESXi-Hypervisor installiert ist. Sie können den Sandbox Analyzer auf mehreren ESXi-Hypervisoren installieren.
- **Detonierte Stichproben.** Der Wert gibt die Gesamtzahl der Stichproben an, die seit der ersten Lizenzierung von Sandbox Analyzer analysiert wurden.
- **Datenträgerverwendung.** Der Prozentsatz gibt den vom Sandbox Analyzer im Datenspeicher belegten Speicherplatz an.
- **Status.** In dieser Spalte sehen Sie, ob die Sandbox Analyzer-Instanz online, offline oder nicht installiert ist, ob die Installation gerade erfolgt oder die Installation fehlgeschlagen ist.
- **Maximale gleichzeitige Detonationen.** Dieser Wert gibt die maximale Anzahl von virtuellen Maschinen an, die von Sandbox Analyzer zur Detonation von Stichproben erstellt werden kann. Eine virtuelle Maschine kann immer nur eine Detonation durchführen. Die Anzahl der virtuellen Maschinen wird durch die auf ESXi verfügbaren Hardware-Ressourcen bestimmt.
- **Konfigurierte gleichzeitige Detonationen.** Dies ist die tatsächliche Anzahl der virtuellen Maschinen, die auf Grundlage auf der verfügbaren Lizenz erstellt wurden.
- **Proxy verwenden.** Klicken Sie auf den An/Aus-Schalter, um die Kommunikation zwischen dem GravityZone Control Center und den Sandbox Analyzer-Instanzen über einen Proxy-Server zu (de)aktivieren. Einrichten können Sie einen

Proxy-Server unter **Konfiguration > Proxy** im Hauptmenü des Control Center. Wenn kein Proxy-Server eingerichtet ist, ignoriert das Control Center diese Option.

Weitere Details zur Konfiguration von Proxy-Servern erfahren Sie unter **Schutz installieren > GravityZone-Installation und -Einrichtung > Control Center-Einstellungen konfigurieren > Proxy** der GravityZone-Installationsanleitung.



Beachten Sie

Das Control Center verwendet diesen Proxy-Server ausschließlich zur Kommunikation mit Instanzen von Sandbox Analyzer On-Premises. Zur Kommunikation mit der Cloud-Instanz von Sandbox Analyzer verwendet das Control Center den in den Richtlinieneinstellungen auf der Seite Sandbox Analyzer konfigurierten Proxy-Server.

Dieser Proxy-Server ist auch ein anderer als der, der auf der Seite **Allgemein > Einstellungen** der Richtlinieneinstellungen konfiguriert ist. Letzterer ist für die Kommunikation zwischen Endpunkten und GravityZone-Komponenten zuständig.

Sie können die Spalten nach Status und Name der Sandbox Analyzer-Instanz durchsuchen und filtern. Über die Schaltflächen rechts oben in der Tabelle können Sie die Seite neu laden sowie Filter und Spalten anzeigen und verbergen.

11.6.2. Konfigurieren gleichzeitiger Detonationen

Auf der Seite **Status** können Sie gleichzeitige Detonationen konfigurieren. Diese entsprechen der Anzahl der virtuellen Maschinen dar, die gleichzeitig Stichproben auf einer Sandbox Analyzer-Instanz ausführen und detonieren können. Die Anzahl der gleichzeitigen Detonationen hängt von den Hardware-Ressourcen und der Verteilung der Lizenzplätze auf den Sandbox Analyzer-Instanzen ab.

Gehen Sie zur Konfiguration gleichzeitiger Detonationen wie folgt vor:

1. Klicken Sie auf die Zahl oder das **Bearbeiten**-Symbol in der Spalte **Konfigurierte gleichzeitige Detonationen**.
2. Ein neues Fenster öffnet sich. Geben Sie im entsprechenden Feld die Anzahl der gleichzeitigen Detonationen an, die Sie für die Sandbox Analyzer-Instanz festlegen möchten.
3. Klicken Sie auf **Speichern**.

11.6.3. Überprüfen des Status des VM-Images

Sandbox Analyzer verwendet virtuelle Maschinen-Images als Detonationsumgebungen, um Verhaltensanalysen für die übermittelten Stichproben durchzuführen. Sie können den Status der virtuellen Maschinen auf der Seite **Image-Verwaltung** überprüfen.

Dashboard		Status Image-Verwaltung				
Netzwerk	Neu laden					
Anwendungsbestand	Name	Betriebssystem	Hinzugefügt	Status	Aktionen	
Pakete	bitdefender-sba-e508					
Aufgaben	___wr10_x64_r91_14393_87tg	os	04 November 2019, 16:41:44	● Bereit	Als Standard einstellen Löschen	
Richtlinien	___wr10_x64_r95_17763_v9_v499	os	04 November 2019, 16:53:51	● Bereit	Als Standard einstellen Löschen	
Zuweisungsregeln	___wr10_x64_r95_17763_v13_u97v	os	04 November 2019, 16:42:24	● Bereit	Als Standard einstellen Löschen	
Berichte	___wr10_x64_r96_8n23	os	04 November 2019, 17:03:22	● Bereit	Als Standard einstellen Löschen	
Quarantäne	___wr10_r94_x64_1sta	os	04 November 2019, 17:02:08	● Bereit	Als Standard einstellen Löschen	
Konten	___wr10_x64_r95_17763_v9_4694	os	04 November 2019, 17:01:32	● Bereit	Als Standard einstellen Löschen	
Richtlinien	___wr10_x64_r95_17763_v12_jd1o	os	04 November 2019, 17:00:57	● Bereit	Als Standard einstellen Löschen	
Zuweisungsregeln	___wr10_x64_r95_17763_v8_83t6	os	04 November 2019, 17:00:13	● Bereit	Als Standard einstellen Löschen	
Berichte	___wr10_x64_r95_17763_v11_38fp	os	04 November 2019, 16:59:21	● Bereit	Als Standard einstellen Löschen	

Sandbox Analyzer > Infrastruktur > Image-Verwaltung

In der Tabelle finden Sie die folgenden Informationen:

- **Name** der verfügbaren virtuellen Maschinen-Images, wie in der Sandbox Analyzer-Appliance-Konsole angegeben. Mehrere virtuelle Maschinen-Images werden unter derselben Sandbox Analyzer-Instanz zusammengefasst.
- **Betriebssystem**, wie in der Sandbox Analyzer-Appliance-Konsole angegeben.
- Der Zeitpunkt, zu dem das virtuelle Maschine-Image hinzugefügt wurde.
- **Status**. Dieser Spalte entnehmen Sie, ob ein virtuelles Maschinen-Image neu ist und für die Detonation vorbereitet werden kann, zur Detonation bereit ist oder der Vorbereitungsprozess fehlgeschlagen ist.
- **Aktionen**. Dieser Spalte entnehmen Sie, was Sie mit den virtuellen Maschinen-Images abhängig von ihrem Status machen können: Erstellen von Images für die Detonation, Festlegen als Standarddetonationsumgebung oder Löschen.

11.6.4. Konfigurieren und Verwalten von VM-Images

Erstellen von virtuellen Maschinen für die Detonation

Um Stichproben mit der lokalen Sandbox Analyzer-Instanz zu detonieren, müssen Sie dedizierte virtuelle Maschinen erstellen. Auf der Seite **Image-Verwaltung** können Sie virtuelle Maschinen für die Detonation erstellen, sofern Sie VM-Images in der Sandbox Analyzer-Appliance-Konsole hinzugefügt haben.



Beachten Sie

Um zu erfahren, wie Sie VM-Images in der Sandbox Analyzer-Appliance-Konsole hinzufügen können, lesen Sie bitte das Kapitel **Installieren der virtuellen Sandbox Analyzer-Appliance** im GravityZone-Installationshandbuch .

Um virtuelle Maschinen für die Detonation zu erstellen, klicken Sie in der Spalte **Aktionen** auf die Option **Build Image** für VM-Images mit dem Status: **Neu - Muss erstellt werden**. Die Erstellung einer virtuellen Maschine dauert je nach Größe zwischen 15 und 30 Minuten. Wenn die Image-Erstellung abgeschlossen ist, ändert sich der Status der virtuellen Maschinen zu **Bereit**.

Konfigurieren einer standardmäßigen virtuellen Maschine

Auf einer Sandbox Analyzer-Instanz können mehrere Images installiert und als virtuelle Maschinen für die Detonation konfiguriert werden. Bei automatischen Übermittlungen verwendet Sandbox Analyzer das zuerst erstellte VM-Image, um Stichproben zu detonieren.

Sie können dieses Verhalten ändern, indem Sie ein standardmäßiges VM-Image konfigurieren. Klicken Sie dazu für das bevorzugte VM-Image auf die Option **Als Standard einstellen**.

Löschen von virtuellen Maschinen

Um ein virtuelles Maschinen-Image von der Seite **Image-Verwaltung** zu löschen, klicken Sie in der Spalte **Aktionen** auf **Löschen**. Klicken Sie im Bestätigungsfenster auf **Image löschen**.

12. BENUTZERAKTIVITÄTSPROTOKOLL

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Die Benutzeraktivitätsliste enthält je nach Ihren Administratorrechten die folgenden Ereignisse:

- Anmelden und Abmelden
- Berichte erstellen, bearbeiten, umbenennen und löschen
- Dashboard-Portlets hinzufügen und entfernen
- Zugangsdaten erstellen, bearbeiten und löschen
- Netzwerkpakete erstellen, modifizieren, herunterladen und löschen
- Netzwerkaufgaben erstellen
- Problembehandlungsvorgänge auf betroffenen Maschinen starten, beenden, abbrechen und anhalten
- Benutzerkonten erstellen, bearbeiten, umbenennen und löschen
- Endpunkte löschen oder zwischen Gruppen verschieben
- Gruppen erstellen, verschieben, umbenennen und löschen
- Dateien aus der Quarantäne löschen oder wiederherstellen
- Benutzerkonten erstellen, bearbeiten und löschen
- Zugriffsberechtigungsregeln erstellen, bearbeiten und löschen.
- Richtlinien erstellen, bearbeiten, umbenennen, zuweisen und löschen
- Bearbeiten der Authentifizierungseinstellungen für die GravityZone-Benutzerkonten.
- Amazon-EC2-Integrationen erstellen, bearbeiten, synchronisieren und löschen
- Microsoft-Azure-Integrationen erstellen, bearbeiten, synchronisieren und löschen
- Die GravityZone-Appliance aktualisieren.

Einzelheiten zu den Benutzeraktivitäten finden Sie auf der Seite **Konten > Benutzeraktivität**, wenn Sie dort die gewünschte Netzwerkansicht aus der [Ansichtsauswahl](#) auswählen.

Dashboard	Benutzer <input type="text"/>	Aktion <input type="text"/>	Ziel <input type="text"/>			Suchen
Netzwerk	Rolle <input type="text"/>	Bereich <input type="text"/>	Erstellt <input type="text"/>	<input type="text"/>	<input type="text"/>	
Pakete	Benutzer	Rolle	Aktion	Bereich	Ziel	Erstellt
Aufgaben						
Richtlinien						
Berichte						
Quarantäne						
Konten						
Benutzeraktivität						
Konfiguration	Erste Seite -- Seite 0 von 0 -- Letzte Seite 20					0 Objekte

Die Seite Benutzeraktivität

Um aufgezeichnete Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie eine Suche definieren. Geben Sie die Suchkriterien in die verfügbaren Felder ein und klicken Sie auf **Suchen**. Alle zu Ihren Kriterien passenden Einträge werden in der Tabelle angezeigt.

Die Spalten geben nützliche Informationen zu den aufgelisteten Ereignissen:

- Der Name des Benutzers, der die Aktion durchgeführt hat.
- Benutzerrolle.
- Aktion, die das Ereignis ausgelöst hat.
- Art des Konsolenobjekts, das von der Aktion betroffen ist.
- Bestimmtes Konsolenobjekt, das von der Aktion betroffen ist.
- Zeitpunkt, zu dem das Ereignis eingetreten ist.

Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

13. VERWENDUNG VON TOOLS

13.1. Benutzerdefiniert Tool-Injektion mit HVI

Bitdefender HVI nimmt Ihnen die Arbeit im Zusammenhang mit der Fehlersuche, der Sammlung von Forensikdaten oder der Ausführung von regelmäßigen Wartungsaufgaben auf den virtuellen Maschinen in Ihrer Citrix-Umgebung ab, indem es Ihnen erlaubt, Drittanbieter-Tools im laufenden Betrieb in die Gast-Betriebssysteme zu injizieren. Diese Vorgänge erfolgen über Direct-Inspect-APIs (es wird keine TCP/IP-Verbindung benötigt), ohne den Endbenutzer in seiner Arbeit zu stören. Zu diesem Zwecke müssen die Tools im Hintergrund ausgeführt werden können.

Mit GravityZone erhalten Sie 3 GB Speicherplatz, um Ihre Tools sicher zu verwahren und sie von dort aus in die Gast-Betriebssysteme zu injizieren.

Gehen Sie folgendermaßen vor, um die Tool-Kits in GravityZone hochzuladen:

1. Laden Sie die aktuelle Kit-Version des Tools auf Ihren Computer herunter.
2. Archivieren Sie das Kit in einer ZIP-Datei.
3. Öffnen Sie das GravityZone Control Center und klicken Sie links unten auf der Seite auf das **Tools**-Menü. Die Seite **Tool-Verwaltungszentrum** wird angezeigt.
4. Klicken Sie oben in der Tabelle je nach Ziel-Betriebssystem auf die entsprechende Upload-Schaltfläche: **Windows-Tool hochladen** oder **Linux-Tool hochladen**.
5. Bei einem Windows-Tool müssen Sie zudem aus dem Klappmenü die entsprechende Computer-Architektur auswählen.
6. Suchen Sie die ZIP-Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**.

Bei größeren Dateien müssen Sie unter Umständen ein paar Minuten warten, bis der Upload abgeschlossen ist. Nach Abschluss wird das Tool der Tabelle hinzugefügt und in der Statusanzeige über der Tabelle werden die Informationen über den verfügbaren Speicherplatz für zukünftige Uploads aktualisiert.

Neben dem Namen des Tools werden in der Tabelle weitere nützliche Details angezeigt, so z. B.:

- Das Betriebssystem und die Plattform, auf dem das Tool läuft.

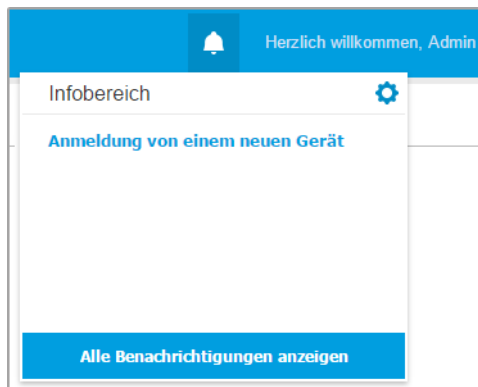
- Eine kurze Beschreibung des Tools. Sie können dieses Feld jederzeit nach Bedarf bearbeiten.
- Der Name des Benutzers, der das Tool hochgeladen hat.
- Upload-Status. In diesem Feld können Sie nachsehen, ob das Tool erfolgreich hochgeladen wurde.
- Datum und Zeitpunkt des Uploads.

Im nächsten Schritt können Sie über Richtlinien planen, wann die Tools injiziert werden sollen oder Sie zu jedem beliebigen Zeitpunkt injizieren, indem Sie Aufgaben über die Seite **Netzwerk** ausführen.


Wenn Sie die Tools nicht mehr länger benötigen, können Sie sie auswählen und mit einem Klick auf die **Löschen**-Schaltfläche oben in der Tabelle wieder entfernen. Klicken Sie zur Bestätigung auf **Ja**.

14. BENACHRICHTIGUNGEN

Je nach den Ereignissen, die in Ihrem Netzwerk auftreten, wird das Control Center verschiedene Benachrichtigungen anzeigen, die Sie über den Sicherheitsstatus Ihrer Umgebung auf dem Laufenden halten. Die Benachrichtigungen werden im **Infobereich** an der rechten Seite des Control Center angezeigt.



Infobereich

Wenn neue Ereignisse im Netzwerk gefunden werden, zeigt das -Symbol oben rechts in der Control Center die Anzahl der gefundenen Ereignisse an. Mit einem Klick auf das Symbol wird der Infobereich mit der Liste der gefundenen Ereignisse angezeigt.

14.1. Benachrichtigungsarten

Hier eine Liste der verfügbaren Benachrichtigungstypen:

Malware-Ausbruch

Diese Benachrichtigung wird an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit derselben Malware infiziert haben.

Im Fenster **Benachrichtigungseinstellungen** können Sie die Malware-Ausbruchschwelle Ihren Bedürfnissen entsprechend konfigurieren. Weitere Informationen finden Sie unter [„Benachrichtigungseinstellungen konfigurieren“](#) (S. 523).

Von HyperDetect gefundene Bedrohungen werden von dieser Benachrichtigung nicht abgedeckt.

Verfügbares Syslog-Format: JSON, CEF

Lizenz läuft ab

Diese Benachrichtigung wird 30, 7 und dann noch einmal einen Tag, bevor die Lizenz abläuft, gesendet.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

Verfügbares Syslog-Format: JSON, CEF

Lizenzobergrenze ist erreicht

Diese Benachrichtigung wird gesendet, wenn alle verfügbaren Lizenzen vergeben sind.

Verfügbares Syslog-Format: JSON, CEF

Benutzergrenze der Lizenz ist bald erreicht

Diese Benachrichtigung wird gesendet, wenn 90 % der verfügbaren Lizenzen vergeben sind.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

Verfügbares Syslog-Format: JSON, CEF

Exchange-Lizenz-Benutzergrenze ist erreicht

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn die Anzahl der auf Ihren Exchange-Servern geschützten Mailboxen die im Lizenzschlüssel festgelegte Grenze erreicht.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

Verfügbares Syslog-Format: JSON, CEF

Ungültige Exchange-Benutzer-Zugangsdaten

Diese Benachrichtigung wird gesendet, wenn eine Bedarf-Scan-Aufgabe aufgrund ungültiger Exchange-Benutzer-Zugangsdaten auf dem gewünschten Exchange-Server nicht gestartet werden konnte.

Verfügbares Syslog-Format: JSON, CEF

Upgrade-Status

Diese Benachrichtigung wird wöchentlich ausgegeben, wenn alte Produktversionen in Ihrem Netzwerk gefunden werden.

Verfügbares Syslog-Format: JSON, CEF

Update verfügbar

Diese Benachrichtigung informiert Sie über eine neue GravityZone-Version, ein neues Paket oder ein neues Produkt-Update.

Verfügbares Syslog-Format: JSON, CEF

Internetverbindung

Diese Benachrichtigung wird ausgegeben, wenn von einem der folgenden Prozesse Schwankungen in der Internetverbindung bemerkt werden:

- Lizenzüberprüfung
- Erhalt einer Anfrage zur Unterzeichnung eines Apple-Zertifikats
- Kommunikation mit Apple- und Android-Mobilgeräten
- Zugriff auf das MyBitdefender-Konto

Verfügbares Syslog-Format: JSON, CEF

SMTP-Verbindung

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn Bitdefender GravityZone Schwankungen in der Mail-Server-Verbindung bemerkt.

Verfügbares Syslog-Format: JSON, CEF

Mobilgerätbenutzer ohne E-Mail-Adresse

Diese Benachrichtigung wird ausgegeben, wenn Mobilgeräte mehreren Benutzern hinzugefügt werden und für mindestens einen der ausgewählten Benutzer keine E-Mail-Adresse in seinem Konto hinterlegt ist. Diese Benachrichtigung weist Sie darauf hin, dass Benutzer ohne hinterlegte E-Mail-Adresse die ihnen zugewiesenen Mobilgeräte nicht registrieren können, da die Aktivierungsdetails automatisch per E-Mail versendet werden.

Näheres dazu, wie Sie Mobilgeräte mehreren Benutzern hinzufügen, finden Sie in der GravityZone-Installationsanleitung.

Verfügbares Syslog-Format: JSON, CEF

Datenbank-Backup

Diese Benachrichtigung informiert Sie über den Status eines geplanten Datenbank-Backups, ob erfolgreich oder unerfolgreich. Wenn das

Datenbank-Backup fehlgeschlagen ist, wird in der Benachrichtigung auch die Ursache für das Fehlschlagen genannt.

Details zur Konfiguration von GravityZone-Datenbank-Backups finden Sie in der GravityZone-Installationsanleitung.

Verfügbares Syslog-Format: JSON, CEF

Exchange-Malware gefunden

Diese Benachrichtigung informiert Sie darüber, dass auf einem Exchange-Server in Ihrem Netzwerk Malware gefunden wurde.

Verfügbares Syslog-Format: JSON, CEF

Erweiterter Exploit-Schutz

Diese Benachrichtigung wird ausgegeben, wenn der erweiterte Exploit-Schutz Exploit-Versuche in Ihrem Netzwerk erkannt hat.

Verfügbares Syslog-Format: JSON, CEF

Malware-Schutz-Ereignis

Diese Benachrichtigung informiert Sie darüber, dass auf einem Endpunkt in Ihrem Netzwerk Malware gefunden wurde. Diese Benachrichtigung wird für jede Malware-Erkennung erstellt und enthält Details über den infizierten Endpunkt (Name, IP, installierter Agent), den Scan-Typ, die gefundene Malware, die Signaturversion, den Zeitpunkt des Fundes und den Scan-Engine-Typ.

Verfügbares Syslog-Format: JSON, CEF

Integration mit Synchronisationsproblem

Diese Benachrichtigung wird ausgegeben, wenn die Synchronisierung zwischen einer bestehenden virtuellen Plattform-Integration und GravityZone nicht möglich war. In den Benachrichtigungseinstellungen können Sie die Integrationen auswählen, für die Sie bei einem Synchronisationsfehler benachrichtigt werden möchten. Weitere Informationen zum Synchronisierungsstatus finden Sie in den Benachrichtigungsdetails.

Verfügbares Syslog-Format: JSON, CEF

Phishing-Schutz-Ereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn der Endpunkt-Agent den Zugriff auf eine bekannte Phishing-Webseite blockiert. Die Benachrichtigungen enthält auch Details wie den Endpunkt, von dem aus versucht wurde, auf die unsichere Webseite zuzugreifen (Name und IP-Adresse), den installierten Agent oder die blockierte URL.

Verfügbares Syslog-Format: JSON, CEF

Firewall-Ereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn das Firewall-Modul eines installierten Agenten einen Port-Scan oder den Zugriff einer Anwendung auf das Netzwerk gemäß der zugewiesenen Richtlinie blockiert hat.

Verfügbares Syslog-Format: JSON, CEF

ATC/IDS-Ereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn eine potenziell gefährliche Anwendung auf einem Endpunkt in Ihrem Netzwerk gefunden und blockiert wurde. Hier finden Sie Einzelheiten zu Anwendungstyp, -name und -pfad sowie ggf. die ID und den Pfad des übergeordneten Prozesses und die Befehlszeile, die den Prozess gestartet hat.

Verfügbares Syslog-Format: JSON, CEF

Benutzersteuerungsereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn der Endpunkt-Client gemäß der zugewiesenen Richtlinie Benutzeraktivitäten wie das Browsen im Internet oder eine Software-Anwendung blockiert.

Verfügbares Syslog-Format: JSON, CEF

Identitätsschutzereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn gemäß den Identitätsschutzregeln Datenverkehr auf einem Endpunkt blockiert wird.

Verfügbares Syslog-Format: JSON, CEF

Produkt-Modul-Ereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn ein Sicherheitsmodul eines installierten Agenten aktiviert oder deaktiviert wird.

Verfügbares Syslog-Format: JSON, CEF

Security Server-Statusereignis

Diese Benachrichtigungen informieren Sie über die Statusveränderungen eines bestimmten Security Servers, der in Ihrem Netzwerk installiert ist. Mit Statusveränderungen eines Security Servers ist hier Folgendes gemeint: eingeschaltet/ausgeschaltet, Produkt-Update, Update der Sicherheitsinhalte und erforderlicher Neustart.

Verfügbares Syslog-Format: JSON, CEF

Security Server-Überlastungsereignis

Diese Benachrichtigung wird gesendet, wenn die Scan-Last eines Security Server in Ihrem Netzwerk die festgelegte Schwelle überschreitet.

Verfügbares Syslog-Format: JSON, CEF

Produktregistrierungsereignis

Diese Benachrichtigung informiert Sie darüber, wenn sich der Registrierungsstatus eines in Ihrem Netzwerk installierten Agenten geändert hat.

Verfügbares Syslog-Format: JSON, CEF

Authentifizierungsüberprüfung

Diese Benachrichtigung wird verschickt, wenn ein GravityZone-Konto, das nicht Ihr eigenes ist, verwendet wurde, um sich über ein unbekanntes Gerät bei Control Center anzumelden.

Verfügbares Syslog-Format: JSON, CEF

Anmeldung von einem neuen Gerät

Diese Benachrichtigung informiert Sie darüber, dass über Ihr GravityZone-Konto eine Anmeldung am Control Center von einem Gerät aus erfolgt ist, von dem aus Sie sich bisher noch nicht angemeldet hatten. Die Benachrichtigung wird automatisch so konfiguriert, dass sie sowohl in der Control Center angezeigt als auch per E-Mail verschickt wird und schreibgeschützt ist.

Verfügbares Syslog-Format: JSON, CEF

Zertifikat läuft ab

Diese Benachrichtigung informiert Sie darüber, dass ein Sicherheitszertifikat abläuft. Die Benachrichtigung wird 30, 7 und 1 Tag(e) vor dem Ablaufdatum gesendet.

Verfügbares Syslog-Format: JSON, CEF

GravityZone-Update

Die Benachrichtigung wird versendet, wenn ein GravityZone-Update abgeschlossen ist. Wenn das Update fehlschlägt, erfolgt in 24 Stunden ein neuer Installationsversuch.

Verfügbares Syslog-Format: JSON, CEF

Aufgabenstatus

Diese Benachrichtigung wird, je nach Ihren Einstellungen, entweder jedes Mal gesendet, wenn sich der Status einer Aufgabe ändert, oder, nur wenn eine Aufgabe abgeschlossen wird.

Verfügbares Syslog-Format: JSON, CEF

Veralteter Update-Server

Diese Benachrichtigung wird gesendet, wenn die Sicherheitsinhalte auf einem Update-Server in Ihrem Netzwerk veraltet sind.

Verfügbares Syslog-Format: JSON, CEF

Netzwerkvorfallereignis

Diese Benachrichtigung wird immer dann ausgegeben, wenn das Network Attack Defense-Modul den Versuch eines Angriffs auf Ihr Netzwerk erkennt. Diese Benachrichtigung informiert Sie auch, ob der Angriffsversuch von außerhalb des Netzwerks oder von einem infizierten Endpunkt innerhalb des Netzwerks aus durchgeführt wurde. Weitere Details umfassen Daten zum Endpunkt, zur Angriffstechnik, die IP des Angreifers und die von Network Attack Defense ergriffenen Maßnahmen.

Verfügbares Syslog-Format: JSON, CEF

Benutzerdefinierter Bericht wurde generiert

Diese Benachrichtigung meldet Ihnen, dass ein abfragebasierter Bericht generiert wurde.

Verfügbares Syslog-Format: N/A

Speicherverletzung erkannt

Diese Benachrichtigung informiert Sie, wenn HVI einen Angriff erkennt, der auf den Speicher der geschützten virtuellen Maschine in der Citrix Xen-Umgebung abzielt. Die Meldung liefert wichtige Informationen wie z.B. Name und IP der infizierten Maschine, Beschreibung des Vorfalls, Quelle und Ziel des Angriffs, ergriffene Maßnahme zur Beseitigung der Bedrohung und Zeitpunkt der Angriffserfassung.

Benachrichtigungen werden für folgende Vorfälle erstellt:

- Versuche über die Extended Page Tables (EPT), den Speicherbereich für andere als vom Hypervisor vorgesehene Zwecke zu verwenden.
- Versuche von Prozessen, Codes in andere Prozesse zu injizieren.
- Versuche, die Prozessadresse in den Übersetzungstabellen zu ändern.

- Versuche, die Model Specific Registers (MSR) zu ändern.
- Versuche, den Inhalt eines bestimmten Treiberobjekts oder der Interrupt Descriptor Table (IDT) zu ändern.
- Versuche, Steuerregister (CR) mit ungültigen Werten zu laden.
- Versuche, bestimmte Extended Control Register (XCR) mit ungültigen Werten zu laden.
- Versuche, die Global oder Interrupt Descriptor Tables zu ändern.



Beachten Sie

Die HVI-Funktion ist in einigen GravityZone-Lösungen über einen separaten Lizenzschlüssel erhältlich.

Verfügbares Syslog-Format: JSON, CEF

Neue Anwendung im Anwendungsbestand

Diese Benachrichtigung wird angezeigt, wenn die Anwendungssteuerung die Installation einer neuen Anwendung auf den überwachten Endpunkten erkannt hat.

Verfügbares Syslog-Format: JSON, CEF

Blockierte Anwendung

Diese Benachrichtigung informiert Sie, wenn die Anwendungssteuerung einen Prozess einer nicht autorisierten Anwendung blockiert hat oder blockieren würde, abhängig von der Konfiguration des Moduls (Produktiv- oder Testmodus).

Verfügbares Syslog-Format: JSON, CEF

Sandbox Analyzer-Erkennung

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn der Sandbox Analyzer unter den übermittelten Stichproben eine neue Bedrohung findet. Angezeigt werden Details wie Hostname oder IP-Adresse des Endpunkts, Datum und Uhrzeit des Fundes, Art der Bedrohung, Pfad, Name und Größe der Dateien und die jeweils ausgeführte Bereinigungsaktion.



Beachten Sie

Sie erhalten keine Benachrichtigungen für Stichproben, die von der Analyse als unbedenklich eingestuft wurden. Informationen zu sämtlichen übermittelten Stichproben stehen im Bericht **Sandbox Analyzer-Ergebnisse (veraltet)** und im Bereich **Sandbox Analyzer** im Hauptmenü des Control Center zur Verfügung.

Verfügbares Syslog-Format: JSON, CEF

Problem durch fehlenden Patch

Diese Benachrichtigung wird angezeigt, wenn auf Endpunkten in Ihrem Netzwerk ein oder mehrere Patches fehlen.

GravityZone sendet automatisch eine Benachrichtigung mit allen Funden der letzten 24 Stunden vor dem Benachrichtigungszeitpunkt.

Sie können überprüfen, für welche Endpunkte dies zutrifft, indem Sie in den Benachrichtigungsdetails auf **Bericht anzeigen** klicken.

Die Benachrichtigung bezieht sich standardmäßig auf sicherheitsrelevante Patches. Sie kann aber auch zur Anzeige von nicht sicherheitsrelevanten Patches konfiguriert werden.

Verfügbares Syslog-Format: JSON, CEF

Ransomware-Fund

Diese Benachrichtigung informiert Sie, wenn GravityZone einen Ransomware-Angriff in Ihrem Netzwerk erkennt. Sie erhalten Angaben über den betroffenen Endpunkt, den angemeldeten Benutzer, die Quelle des Angriffs, die Anzahl der verschlüsselten Dateien sowie Zeit und Datum des Angriffs.

Zum Zeitpunkt der Benachrichtigung wurde der Angriff bereits blockiert.

Der Link in der Benachrichtigung leitet Sie auf die Seite **Ransomware-Aktivität** weiter. Hier können Sie eine Liste der verschlüsselten Dateien einsehen und diese bei Bedarf wiederherstellen.

Verfügbares Syslog-Format: JSON, CEF

Speicher-Malware-Schutz

Diese Benachrichtigung wird gesendet, wenn Malware auf einem ICAP-konformen Speichergerät gefunden wird. Die Benachrichtigung wird bei jedem Malware-Fund ausgegeben, und enthält Details zum infizierten Endpunkt (Name, IP-Adresse, Art), zur gefundenen Malware sowie den Zeitpunkt des Fundes.

Verfügbares Syslog-Format: JSON, CEF


Blockierte Geräte

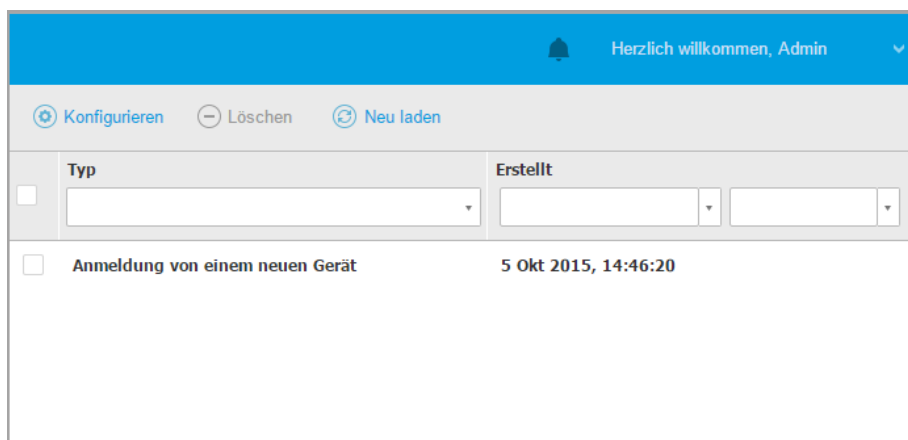
Diese Benachrichtigung wird ausgegeben, wenn sich ein blockiertes Gerät oder ein Gerät mit Leseberechtigung mit dem Endpunkt verbindet. Wenn das gleiche Gerät innerhalb einer Stunde mehrere Verbindungen aufbaut, wird in diesem Zeitraum nur eine Benachrichtigung ausgegeben. Wenn das Gerät nach Ablauf

der Stunde erneut eine Verbindung aufbaut, wird eine neue Benachrichtigung ausgegeben.

Verfügbares Syslog-Format: JSON, CEF

14.2. Benachrichtigungen anzeigen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche  **Benachrichtigungen** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.



	Typ	Erstellt
<input type="checkbox"/>		
<input type="checkbox"/>	Anmeldung von einem neuen Gerät	5 Okt 2015, 14:46:20

Die Benachrichtigungsübersicht

Abhängig von der Anzahl der Benachrichtigungen kann sich die Tabelle über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.

Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das Filtermenü über der Tabelle verwenden, um die angezeigten Daten zu filtern.



- Sie können die Benachrichtigungen filtern, indem Sie den gewünschten Benachrichtigungstyp aus dem Menü **Typ** wählen. Optional können Sie auch

den Zeitraum, in dem die Benachrichtigungen erstellt wurden, eingrenzen, um die Zahl der in der Tabelle angezeigten Einträge zu verringern, besonders wenn sehr viele Benachrichtigungen erstellt worden sind.

- Wenn Sie auf den Namen einer Benachrichtigung in der Tabelle klicken, werden weitere Details zu ihr angezeigt. Unter der Tabelle wird der Bereich **Details** angezeigt, in dem das Ereignis angezeigt wird, dass die Benachrichtigung verursacht hat.

14.3. Benachrichtigungen löschen

So löschen Sie Benachrichtigungen:



1. Klicken Sie auf der rechten Seite der Menüleiste auf die Schaltfläche  **Benachrichtigung** und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Wählen Sie die Benachrichtigungen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche  **Löschen** am oberen Rand der Tabelle.

Sie können auch einstellen, dass Benachrichtigungen nach einer bestimmten Anzahl an Tagen gelöscht werden. Weitere Informationen finden Sie unter „[Benachrichtigungseinstellungen konfigurieren](#)“ (S. 523).

14.4. Benachrichtigungseinstellungen konfigurieren

Die Benachrichtigungstypen, die gesendet werden, sowie die E-Mail-Adresse, an die sie gesendet werden, können für jeden Benutzer einzeln festgelegt werden.

So konfigurieren Sie die Benachrichtigungseinstellungen:

1. Klicken Sie auf der rechten Seite der Menüleiste auf die Schaltfläche  **Benachrichtigung** und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Klicken Sie auf die Schaltfläche  **Konfigurieren** am oberen Rand der Tabelle. Das Fenster **Benachrichtigungseinstellungen** wird angezeigt.

Benachrichtigungseinstellungen




Beachten Sie

Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das  **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

- Im Bereich **Konfiguration** können Sie die folgenden Einstellungen vornehmen:
 - Benachrichtigungen automatisch nach Ablauf einer bestimmten Zeit löschen. Eine beliebige Zahl zwischen 0 und 365 ins Feld **Benachrichtigungen nach (Tagen) löschen** eintragen.
 - Wählen Sie das Kästchen **Neue-Lade-Benachrichtigungen aktivieren**, wenn der Infobereich automatisch alle 60 Sekunden aktualisiert werden soll.
 - Zusätzlich können Sie die Benachrichtigungen per E-Mail an bestimmte Empfänger schicken. Geben Sie die E-Mail-Adressen in das vorgesehene Feld ein und drücken Sie nach jeder Adresse **Eingabe**.
- Im Bereich **Benachrichtigung aktivieren** können Sie festlegen, welche Art von Benachrichtigungen Sie von GravityZone erhalten möchten. Sie können auch für jeden Benachrichtigungstyp einzeln die Anzeige- und Versandoptionen festlegen.

Wählen Sie einen Benachrichtigungstyp aus der Liste. Weitere Informationen finden Sie unter „[Benachrichtigungsarten](#)“ (S. 513). Solange ein Benachrichtigungstyp ausgewählt ist, können Sie auf der rechten Seite die Optionen (sofern vorhanden) für diesen Typ konfigurieren:

Transparenz

- **Im Control Center anzeigen** legt fest, dass dieser Ereignistyp im Control Center über die Schaltfläche  im **Benachrichtigungen** angezeigt wird.
- **Protokoll an Server senden** legt fest, dass dieser Ereignistyp auch an die Syslog-Datei geschrieben wird, falls ein Syslog konfiguriert ist.
Näheres dazu, wie Sie Syslog-Server konfigurieren, finden Sie in der GravityZone-Installationsanleitung.
- **per E-Mail senden:** Dieser Ereignistyp wird auch an bestimmte E-Mail-Adressen gesendet. In diesem Fall müssen Sie die E-Mail-Adressen in das entsprechende Feld eingeben und nach jeder Adresse die `Enter`-Taste drücken.

Konfiguration

- **Benutzerdefinierte Schwelle verwenden** - hiermit kann eine Schwelle für die eingetretenen Ereignisse festgelegt werden, für die die ausgewählte Benachrichtigung gesendet wird.
Zum Beispiel wird die Malware-Ausbruch-Benachrichtigung standardmäßig an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit der gleichen Malware infiziert haben. Sie können die Malware-Ausbruchschwelle verändern, indem Sie die Option **Benutzerdefinierte Schwelle verwenden** aktivieren und dann den gewünschten Wert in das Feld **Malware-Ausbruchschwelle** eingeben.
- Wenn Sie möchten, werden Sie nur dann benachrichtigt, wenn ein **Datenbank-Backup** fehlgeschlagen ist. Entfernen Sie die Markierung dieser Option, wenn Sie über alle Ereignisse benachrichtigt werden möchten, die mit Datenbank-Backups zusammenhängen.
- Für **Security Server-Status-Ereignis** können Sie die Security Server-Ereignisse wählen, die diesen Typ von Benachrichtigung auslösen:

- **Veraltet** - gibt jedes Mal eine Benachrichtigung aus, wenn ein Security Server in Ihrem Netzwerk veraltet ist.
 - **Ausgeschaltet** - gibt jedes Mal eine Benachrichtigung aus, wenn Security Server in Ihrem Netzwerk heruntergefahren wurde.
 - **Neustart erforderlich** - gibt jedes Mal eine Benachrichtigung aus, wenn ein Security Server in Ihrem Netzwerk neu gestartet werden muss.
 - Für **Aufgabenstatus** können Sie den Typ des Status wählen, der diesen Typ von Benachrichtigung auslöst:
 - **Jeden Status** - gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe ausgeführt wurde, unabhängig vom Status.
 - **Nur fehlgeschlagene** – gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe fehlgeschlagen ist.
5. Klicken Sie auf **Speichern**.

15. SYSTEMSTATUS

Auf der Seite **Systemstatus** werden Informationen zum Systemzustand der GravityZone-Bereitstellung angezeigt, so dass Sie auf den ersten Blick erkennen können, ob es Probleme gibt. Auf dieser Seite finden Sie in einer Rasterdarstellung Systemkennzahlen, Statusinformationen und den Zeitpunkt der letzten Aktualisierung.

Metrics	Last Updated	Status
Web Console Data Processors	18 February 2020, 19:45:08	OK
Disk Usage	18 February 2020, 19:45:08	Warning
Communication Server	18 February 2020, 19:45:08	OK
Database Server	18 February 2020, 19:45:08	OK
Web Server	18 February 2020, 19:45:08	OK
Message Broker	18 February 2020, 19:45:08	Warning

Systemstatusseite

In der Spalte **Metriken** werden alle Kennzahlen angezeigt, die von der GravityZone Control Center überwacht werden. Weitere Informationen zu Kennzahlen und Statusmeldungen finden Sie im Abschnitt „Datenprozessoren“ (S. 551).

Die Spalte **Letztes Update** zeigt Datum und Uhrzeit der letzten Statusprüfung der Kennzahl an.

Die Spalte **Status** zeigt den Status jeder Kennzahl an: OK oder **Achtung**. Der **Status** einer Kennzahl wird alle 15 Minuten oder jedes Mal aktualisiert, wenn Sie auf die Schaltfläche **Neu laden** klicken.

15.1. Status OK

Der Status OK zeigt an, dass sich die Kennzahl normal verhält. In diesem Fall werden keine weiteren Informationen angezeigt.

15.2. Status Achtung

Der Status Achtung zeigt an, dass die Metrik nicht innerhalb der normalen Parameter läuft.

In diesem Fall müssen Sie näher untersuchen, was passiert ist und die vorliegenden Probleme beheben:

1. Klicken Sie auf die Schaltfläche **Details**, um zusätzliche Informationen zu der untersuchten Kennzahl anzuzeigen.

Metrics		Last Updated	Status	
Database Server		09 October 2019, 08:47:08		Details ^
Appliance	Details			
10.17.44.111	The service is inactive since Wed 2019-10-09 08:46:52 UTC; 13s ago			

Weitere Kennzahleninformationen

- Unter **Appliance** finden Sie die IP-Adressen der betroffenen Maschinen.
 - Unter **Details** können Sie die für jede Kennzahl spezifischen Informationen einsehen.
2. Klicken Sie auf **Beheben**, um die Metrik zu reparieren und GravityZone kümmert sich um alles Weitere.

Database Server				Details ^	Fix
Appliance	Details				
10.17.43.29	The service is inactive since Mon 2020-02-17 16:09:29 UTC; 5min ago				

Weitere Kennzahleninformationen

Der Status der Metrik wird nach Behebung des Problems wieder als OK angezeigt.



Beachten Sie

Für alle darüber hinausgehenden Probleme in Zusammenhang mit Metriken wenden Sie sich an das [Enterprise Support Team](#).

15.3. Metriken

Auf der Seite **System Status** finden Sie Details zu den folgenden Kennzahlen:

- [Web-Konsolendatenverarbeitung](#)
- [Datenträgerverwendung](#)
- [Kommunikationsserver](#)
- [Datenbank-Server](#)
- [Web-Server](#)
- [Message Broker](#)

Web-Konsolendatenverarbeitung

Diese Kennzahl überwacht den Zustand der Datenprozessoren, die für die Zusammenstellung der im Control Center angezeigten Daten verwendet werden.

Benachrichtigung zum Status Achtung	Details
Verarbeitungsmodule, die auf dieser Appliance fehlgeschlagen sind: <Eine Reihe von Datenprozessoren> .	Ein oder mehrere Datenprozessoren wurden angehalten.
Die virtuelle Appliance läuft nicht	Die virtuelle Appliance, die Dienste der Web-Konsole verwendet, wurde heruntergefahren.

Eine vollständige Liste der vom Control Center verwendeten Prozessoren finden Sie unter „[Datenprozessoren](#)“ (S. 551).

Datenträgerverwendung

Diese Kennzahl überwacht den von jeder virtuellen Appliance verwendeten Speicherplatz, den verfügbaren freien Speicherplatz sowie den insgesamt auf der

Festplatte verfügbaren Speicherplatz. Steigt die Festplattennutzung über 80 %, zeigt die Kennzahl den Status **Achtung** an.

Benachrichtigung	zum	Status	Details
Achtung			
Belegter Speicherplatz auf (Datenträgername)			Eine oder mehrere Festplatten werden über 80 % ihrer maximalen Kapazität verwendet.
Die virtuelle Appliance läuft nicht			Die gemeldete virtuelle Appliance wurde heruntergefahren.

Kommunikationsserver

Diese Kennzahl überwacht die Verbindung zwischen den auf Ihren Endpunkten installierten Sicherheitsagenten und dem Datenbank-Server.

Benachrichtigung	zum	Status	Achtung	Details
Der Dienst ist inaktiv seit <timestamp>				Der Dienst läuft nicht mehr.

Datenbank-Server

Diese Kennzahl überwacht den Status der GravityZone-Datenbank.

Benachrichtigung	zum	Status	Details
Achtung			
Der Dienst ist inaktiv seit <timestamp>			Der Dienst läuft auf einem der Appliances nicht mehr.
Die virtuelle Appliance läuft nicht			Die virtuelle Appliance, die den Datenbank-Server verwendet, wurde heruntergefahren.

Web-Server

Diese Kennzahl überwacht den Zustand des Web-Servers, der das GravityZone Control Center hostet.



Benachrichtigung	zum	Status	Details
Der Dienst ist inaktiv seit <timestamp>			Der Server läuft auf einer der Appliances nicht mehr.
Die virtuelle Appliance läuft nicht			Die virtuelle Appliance, die diesen Server verwendet, wurde heruntergefahren.

Message Broker

Diese Kennzahl überwacht den Status des Message-Broker-Dienstes auf Appliances mit den Rollen Web-Konsole und Kommunikations-Server.

Benachrichtigung	zum	Status	Achtung	Details
Auf diesen Appliances läuft der Message-Broker-Dienst nicht				Der Dienst läuft auf einem der Appliances nicht mehr.
Die Netzwerkverbindung zwischen Appliances ist abgebrochen				Die Verbindung zwischen zwei Appliances wurde unterbrochen.
Die virtuelle Appliance läuft nicht				Die virtuelle Appliance, die diesen Dienst verwendet, wurde heruntergefahren.

16. HILFE ERHALTEN

Bitdefender hat es sich zur Aufgabe gemacht, seinen Kunden beispiellos schnellen und sorgfältigen Support zu bieten. Sollten Probleme im Zusammenhang mit Ihrem Bitdefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser [Online-Support-Center](#). Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können. Sie können auch das Kundenbetreuungs-Team von Bitdefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.



Beachten Sie

Im Support-Center finden Sie weiterführende Informationen zu unseren Support-Leistungen und Support-Richtlinien.

16.1. Bitdefender-Support-Center

Im [Bitdefender-Support-Center](#) finden Sie alle Hilfe und Informationen rund um Ihr Bitdefender-Produkt.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- Artikel in der Wissensdatenbank
- Bitdefender-Support-Forum
- Produktdokumentation

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Artikel in der Wissensdatenbank

Die Bitdefender-Wissensdatenbank ist eine Online-Datenbank mit Informationen rund um die Bitdefender-Produkte. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender-Wissensdatenbank ist öffentlich zugänglich und komplett durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und

stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigten Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Wissensdatenbank wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Die Bitdefender-Wissensdatenbank für Unternehmensprodukte steht Ihnen jederzeit unter <http://www.bitdefender.de/support/business.html> zur Verfügung.

Bitdefender-Support-Forum

Das Bitdefender-Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, schnelle Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr Bitdefender-Produkt posten.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter <http://forum.bitdefender.com>. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Am einfachsten gelangen Sie über die Seite **Hilfe & Support** im Control Center zur Dokumentation. Klicken Sie oben rechts in der Konsole auf Ihren Benutzernamen, dann auf **Hilfe & Support** und schließlich auf den Link des gewünschten Handbuchs. Dadurch wird ein neuer Reiter in Ihrem Browser geöffnet.

Sie können die Dokumentation auch im [Support-Center](#) im Bereich **Dokumentation**, der auf jeder Produktseite verfügbar ist, einsehen und herunterladen.

16.2. Hilfe anfordern

Nutzen Sie unser Online-Support-Center, um Unterstützung anzufordern. Füllen Sie das [Kontaktformular](#) aus und senden Sie es ab.

16.3. Verwenden des Support-Tools

Das Support-Tool von GravityZone ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Problembehandlung benötigen. Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Problembehandlung an einen Bitdefender-Support-Mitarbeiter.

16.3.1. Das Support-Tool unter Windows verwenden

Ausführen des Support-Tools

Sie haben folgende Möglichkeiten, das Protokoll auf einem betroffenen Computer zu erzeugen:

- **Befehlszeile**
Bei Problemen, wenn BEST auf dem Computer installiert ist.
- **Installationsproblem**
Für den Fall, dass BEST nicht auf dem Computer installiert ist und die Installation fehlschlägt.

Über die Befehlszeile

Über die Kommandozeile können Sie Protokolle direkt auf dem betroffenen Computer erfassen. Diese Methode ist dann besonders nützlich, wenn Sie keinen Zugriff auf das GravityZone-Control Center haben oder der Computer nicht mit der Konsole kommuniziert.

1. Öffnen Sie die PowerShell als Administrator.
2. Wechseln Sie zum Installationsordner des Produkts. Der Standardpfad ist:
`C:\Programme\Bitdefender\Endpoint Security`
3. Führen Sie den folgenden Befehl aus:

```
Product.Support.Tool.exe collect
```

Dadurch werden die Protokolle erzeugt und standardmäßig unter `C:\Windows\Temp` gespeichert.

Wenn Sie die Protokolle lieber in einem anderen Ordner speichern möchten, passen Sie die obige Zeile wie folgt an:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Beispiel:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Während der Befehl ausgeführt wird, wird auf dem Bildschirm ein Fortschrittsbalken angezeigt. Wenn der Vorgang abgeschlossen ist, wird der Name und Speicherort des Archivs angezeigt, das die Protokolle enthält.

Um die Protokolle an den Bitdefender Enterprise Support zu übermitteln, rufen Sie `C:\Windows\Temp` bzw. den benutzerdefinierten Speicherort aus und suchen Sie die Archivdatei mit dem Namen `ST_[computername]_[currentdate]`. Fügen Sie das Archiv zur weiteren Problembehandlung als Anhang Ihrem Support-Ticket hinzu.

Installationsproblem

1. Klicken Sie [hier](#), um das BEST Support Tool herunterzuladen.
2. Führen Sie die ausführbare Datei als Administrator aus. Es wird ein neues Fenster angezeigt.
3. Wählen Sie einen Speicherort zum Speichern des Protokollarchivs.

Während die Protokolle erfasst werden, wird ein Fortschrittsbalken auf dem Bildschirm angezeigt. Wenn der Vorgang abgeschlossen ist, wird der Name und Speicherort des Archivs angezeigt.

Um die Protokolle an den Bitdefender Enterprise Support zu übermitteln, rufen Sie den ausgewählten Speicherort aus und suchen Sie die Archivdatei mit dem Namen `ST_[computername]_[currentdate]`. Fügen Sie das Archiv zur weiteren Problembehandlung als Anhang Ihrem Support-Ticket hinzu.

16.3.2. Das Support-Tool unter Linux

Für Linux-Betriebssysteme ist das Support-Tool im Bitdefender-Sicherheitsagenten integriert.

Linux-Systeminformationen können Sie über das Support-Tool mit dem folgenden Befehl erhalten:

```
# /opt/BitDefender/bin/bdconfigure
```

Dabei stehen folgende Optionen zur Verfügung:

- `--help` zeigt eine Liste aller Support-Tool-Befehle an.
- `enablelogs` aktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `disablelogs` deaktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `deliverall` erstellt
 - ein Archiv, das die Produkt- und Kommunikationsmodul-Protokolle enthält. Es wird an den Ordner `/tmp` im folgenden Format zugestellt:
`Bitdefender_Maschinename_Zeitstempel.tar.gz`.

Nach dem das Archiv erstellt wurde:

1. Wenn Sie die Protokolle deaktivieren möchten, werden Sie um eine Bestätigung gebeten. Wenn nötig, werden die Dienste automatisch neu gestartet.
 2. Wenn Sie Protokolle löschen möchten, werden Sie um eine Bestätigung gebeten.
- Alle `zustellen -standard` liefert dieselben Informationen wie die vorherige Option, Standardaktionen werden jedoch auf die Protokolle ausgeführt, ohne dass der Benutzer dies bestätigt (die Protokolle werden deaktiviert und gelöscht).

Sie können auch den Befehl `/bdconfigure` direkt aus dem BEST-Paket (vollständig oder Downloader) ausführen, ohne dass das Produkt installiert sein muss.

So melden Sie ein GravityZone-Problem, das Ihre Linux-Systeme beeinträchtigt (verwenden Sie dazu die oben beschriebenen Optionen):

1. Aktivieren Sie Produkt- und Kommunikationsmodulprotokolle.

2. Versuchen Sie, das Problem nachzustellen.
3. Deaktivieren Sie Protokolle.
4. Erstellen Sie ein Protokollarchiv.
5. Öffnen Sie ein E-Mail-Support-Ticket über das Formular auf der Seite **Hilfe & Support** des Control Center; geben Sie eine Beschreibung des Problems ein und hängen Sie das Protokollarchiv an.

Das Support-Tool für Linux liefert die folgenden Informationen:

- Die Ordner `etc`, `var/log`, `/var/crash` (sofern vorhanden) und `var/epag` von `/opt/BitDefender`; darin sind die Bitdefender-Protokolle und -Einstellungen enthalten.
- Die Datei `/var/log/BitDefender/bdinstall.log`, die Informationen zu Installation enthält
- Die Datei `network.txt`, die Netzwerkeinstellungen und Informationen zur Netzwerkverbindung der Maschine enthält.
- Die Datei `product.txt`, die sämtliche Inhalte aller `update.txt`-Dateien aus `/opt/BitDefender/var/lib/scan` und eine rekursive vollständige Liste aller Dateien aus `/opt/BitDefender` enthält
- Die Datei `system.txt`, die allgemeine Systeminformationen enthält (Distribution und Kernel-Version, verfügbarer RAM und freier Festplattenspeicher)
- Die Datei `users.txt`, die Benutzerinformationen enthält
- Andere Informationen zum Produkt im Zusammenhang mit dem System, z. B. externe Verbindungen von Prozessen und CPU-Auslastung
- Systemprotokolle

16.3.3. Das Support-Tool unter Mac verwenden

Wir benötigen folgende Angaben für jede Anfrage an den technischen Support von Bitdefender:

- Eine detaillierte Beschreibung des aufgetretenen Problems.
- Gegebenenfalls einen Screenshot von der angezeigten Fehlermeldung.
- Das Support-Tool-Protokoll.

So können Sie mit dem Support-Tool Informationen zu Ihrem Mac-System einholen:

1. Laden Sie das [ZIP-Archiv](#) mit dem Support-Tool herunter.
2. Extrahieren Sie die **BDProfiler.tool**-Datei aus dem Archiv.
3. Öffnen Sie ein Terminalfenster.
4. Öffnen Sie den Speicherort der Datei **BDProfiler.tool**.

Zum Beispiel:

```
cd /Users/Bitdefender/Desktop;
```

5. Fügen Sie der Datei Ausführberechtigungen hinzu:

```
chmod +x BDProfiler.tool;
```

6. Führen Sie das Tool aus.

Zum Beispiel:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Drücken Sie **J** und geben Sie das Kennwort ein, wenn Sie zur Eingabe des Administrator Kennworts aufgefordert werden.

Warten Sie einige Minuten, bis das Tool das Protokoll erstellt hat. Die entsprechende Archivdatei (**Bitdefenderprofile_output.zip**) finden Sie dann auf Ihrem Desktop.

16.4. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 18 Jahren überbietet Bitdefender konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

16.4.1. Internet-Adressen

Vertrieb: enterprisesales@bitdefender.com

Support-Center: <http://www.bitdefender.de/support/business.html>

Dokumentation: gravityzone-docs@bitdefender.com
Lokale Vertriebspartner: <http://www.bitdefender.de/partners>
Partnerprogramm: partners@bitdefender.com
Presse: presse@bitdefender.de
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Website: <http://www.bitdefender.com>

16.4.2. Händler vor Ort

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu <http://www.bitdefender.de/partners>.
2. Öffnen Sie die **Partner-Suche**.
3. Die Kontaktinformationen zum örtlichen Bitdefender Distributor sollten automatisch eingeblendet werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

16.4.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

USA

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Telefon (Vertrieb&Technischer Support): 1-954-776-6262

Vertrieb: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Support-Center: <http://www.bitdefender.com/support/business.html>

Frankreich

Bitdefender

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Telefon: +33 (0)1 47 35 72 73

E-Mail: b2b@bitdefender.fr

Website: <http://www.bitdefender.fr>

Support-Center: <http://www.bitdefender.fr/support/business.html>

Spanien

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28

Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15

Telefon (Technischer Support): (+34) 93 502 69 10

Vertrieb: comercial@bitdefender.es

Website: <http://www.bitdefender.es>

Support-Center: <http://www.bitdefender.es/support/business.html>

Deutschland

Bitdefender GmbH

Technologiezentrum Schwerte

Lohbachstrasse 12

D-58239 Schwerte

Deutschland

Telefon (Geschäftsstelle&Vertrieb): +49 (0) 2304 94 51 60

Telefon (Technischer Support): +49 (0) 2304 99 93 004

Vertrieb: firmenkunden@bitdefender.de

Website: <http://www.bitdefender.de>

Support-Center: <http://www.bitdefender.de/support/business.html>

Großbritannien und Irland

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Telefon (Vertrieb&Technischer Support): (+44) 203 695 3415

E-Mail: info@bitdefender.co.uk

Vertrieb: sales@bitdefender.co.uk

Website: <http://www.bitdefender.co.uk>

Support-Center: <http://www.bitdefender.co.uk/support/business.html>

Rumänien

BITDEFENDER SRL

Orhideea Towers

15A Orhideelor Street

060071 Bucharest, Sector 6

Fax: +40 21 2641799

Telefon (Vertrieb&Technischer Support): +40 21 2063470

Vertrieb: sales@bitdefender.ro

Website: <http://www.bitdefender.ro>

Support-Center: <http://www.bitdefender.ro/support/business.html>

Vereinigte Arabische Emirate

Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Telefon (Vertrieb&Technischer Support): 00971-4-4588935 / 00971-4-4589186

Fax: 00971-4-44565047

Vertrieb: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Support-Center: <http://www.bitdefender.com/support/business.html>

A. Anhänge

A.1. Unterstützte Dateitypen

Die Malware-Scan-Engines der Bitdefender-Sicherheitslösungen können sämtliche Dateitypen scannen, in denen Bedrohungen versteckt sein könnten. Die folgende Liste zeigt die am häufigsten gescannten Dateitypen.

```
{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde;
accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain;
air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax;
bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm;
cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh;
dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with
HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4;
dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget;
gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt;
iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif;
jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf;
mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml;
mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg;
msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx;
odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak;
pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot;
potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz;
prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz;
py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm;
rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr;
script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm;
snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2;
td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa;
url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm;
wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws;
ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;
```

xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Netzwerkobjekttypen und -status

A.2.1. Netzwerkobjekttypen

Jeder einzelne Objekttyp auf der Seite **Netzwerk** wird durch ein eigenes Symbol dargestellt.

In der folgenden Tabelle sind alle Symbole und dazugehörigen Objekttypen aufgeführt.

Symbol	Typ
	Netzwerkgruppe
	Computer
	Relais-Computer
	Exchange-Server-Computer
	Relais-Exchange-Server-Computer
	Virtuelle Maschine
	Relais-VM
	Golden Image
	Virtuelle Exchange-Server-Maschine
	Virtuelle Relais-Exchange-Server-Maschine
	Virtuelle Maschine mit vShield
	Virtuelle Relais-Maschine mit vShield
	Nutanix-Inventar
	Nutanix Prism
	Nutanix-Cluster
	VMware-Inventar
	VMware vCenter
	VMware-Rechenzentrum

Symbol	Typ
	VMware-Ressourcenpool
	VMware-Cluster
	Citrix-Inventar
	XenServer
	Xen Pool
	Amazon-EC2-Inventar
	Amazon-EC2-Integration
	Amazon-EC2-/Microsoft-Azure-Region
	Amazon-EC2-/Microsoft-Azure-Verfügbarkeitszone
	Microsoft-Azure-Inventar
	Microsoft-Azure-Integration
	Security Server
	Security Server mit vShield
	Host ohne Security Server
	Host mit Security Server
	VMware vApp
	Mobilgerätebenutzer
	Mobiles Gerät

A.2.2. Netzwerkobjektstatus

Jedes Netzwerkobjekt hat einen bestimmten Status in Bezug auf Verwaltungszustand, Sicherheitsprobleme, Netzwerkverbindung usw. In der folgenden Tabelle sind alle Statussymbole und ihre Beschreibung aufgeführt.



Beachten Sie

Die unten stehende Tabelle enthält ein paar generische Statusbeispiele. Dieselben Status können, einzeln oder in Kombination, auch bei anderen Netzwerkobjekttypen wie Netzwerkgruppen, Computer usw. auftreten.

Symbol	Status
	Host ohne Security Server, nicht verbunden
	Virtuelle Maschine, offline, nicht verwaltet
	Virtuelle Maschine, online, nicht verwaltet
	Virtuelle Maschine, online, verwaltet
	Virtuelle Maschine, online, verwaltet, mit Problemen
	Virtuelle Maschine, Neustart ausstehend
	Virtuelle Maschine, gesperrt
	Virtuelle Maschine, gelöscht

A.3. Anwendungsdateitypen

Die Malware-Prüf-Engines von Bitdefender-Sicherheitslösungen können so eingerichtet werden, dass nur Anwendungsdateien geprüft werden. Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.

Diese Kategorie beinhaltet Dateien mit folgenden Endungen:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk;

ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsfm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.4. Dateitypen für die Anhangsfilterung

Das Inhaltssteuerungsmodul von Security for Exchange kann E-Mail-Anhänge nach Dateitypen filtern. Die dafür im Control Center verfügbaren Dateiendungen sind:

Ausführbare Dateien

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Bilder

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archive

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Tabellenkalkulationsdateien

fm3; ods; wk1; wk3; wks; xls; xlsx

Präsentationen

odp; pps; ppt; pptx

Dokumente

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Systemvariablen

Für einige der in der Konsole verfügbaren Einstellungen müssen Sie zunächst den Pfad auf dem Ziel-Computern angeben. Es empfiehlt sich, (nach Möglichkeit)

Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

Im Folgenden finden Sie eine Liste der vordefinierten Systemvariablen:

%ALLUSERSPROFILE%

Der Profilordner für alle Benutzer. Typischer Pfad:

C:\Dokumente und Einstellungen\Alle Benutzer

%APPDATA%

Der Anwendungsdatenordner des angemeldeten Benutzers. Typischer Pfad:

C:\Benutzer\{username}\AppData\Roaming

%LOCALAPPDATA%

Temporäre Dateien von Anwendungen. Typischer Pfad:

C:\Benutzer\{username}\AppData\Lokal

%PROGRAMFILES%

Der Programmdateienordner. Meist zu finden unter C:\Programme.

%PROGRAMFILES(X86)%

**Der Programme-Ordner für 32-Bit-Anwendungen (auf 64-Bit-Systemen).
Typischer Pfad:**

C:\Programmdateien (x86)

%COMMONPROGRAMFILES%

Der Ordner Gemeinsame Dateien. Typischer Pfad:

C:\Programmdateien\Gemeinsame Dateien

%COMMONPROGRAMFILES(X86)%

**Der Ordner Gemeinsame Dateien für 32-Bit-Anwendungen (auf 64-Bit-Systemen).
Typischer Pfad:**

C:\Programmdateien (x86)\Gemeinsame Dateien

%WINDIR%

**Der Windows SDateverzeichnis oder SYSROOT. Meist zu finden unter
C:\Windows.**

%USERPROFILE%

Der Pfad zum Profilordner des Benutzers. Typischer Pfad:

```
C:\Benutzer\{username}
```

Unter macOS entspricht der Profilordner des Benutzers dem Home-Ordner. Verwenden Sie zur Konfiguration von Ausschlüssen `$HOME` oder `~`.

A.6. Tools der Anwendungssteuerung

Um die Regeln der Anwendungssteuerung anhand des Hash-Werts der ausführbaren Datei oder des Zertifikatfingerabdrucks festzulegen, müssen Sie zunächst die folgenden Tools herunterladen:

- **Fingerprint**, um den Hash-Wert zu ermitteln.
- **Thumbprint**, um den Wert des Zertifikatfingerabdrucks zu ermitteln.

Fingerprint

Klicken Sie [hier](#) um die ausführbare Fingerprint-Datei herunterzuladen oder rufen Sie folgende Seite auf <http://download.bitdefender.com/business/tools/ApplicationControl/>

So können Sie den Hash-Wert der Anwendung ermitteln:

1. Öffnen Sie das Fenster für die **Eingabeaufforderung**.
2. Öffnen Sie das Verzeichnis mit dem Fingerprint-Tool. Zum Beispiel:

```
cd/users/fingerprint.exe
```

3. Geben Sie den folgenden Befehl ein, um den Hash-Wert einer Anwendung anzuzeigen:

```
fingerprint <application_full_path>
```

4. Rufen Sie die Control Center wieder auf und konfigurieren Sie die Regel anhand des ermittelten Werts. Weitere Informationen finden Sie unter „Anwendungssteuerung“ (S. 355).

Thumbprint

Klicken Sie [hier](#) um die ausführbare Thumbprint-Datei herunterzuladen oder rufen Sie [folgende Seite](http://download.bitdefender.com/business/tools/ApplicationControl/) auf <http://download.bitdefender.com/business/tools/ApplicationControl/>

So können Sie den Zertifikatfingerabdruck ermitteln:

1. Öffnen Sie die **Eingabeaufforderung** als Administrator.
2. Öffnen Sie das Verzeichnis mit dem Thumbprint-Tool. Zum Beispiel:

```
cd/users/thumbprint.exe
```

3. Geben Sie den folgenden Befehl ein, um den Zertifikatfingerabdruck anzuzeigen:

```
thumbprint <application_full_path>
```

4. Rufen Sie die Control Center wieder auf und konfigurieren Sie die Regel anhand des ermittelten Werts. Weitere Informationen finden Sie unter „Anwendungssteuerung“ (S. 355).

A.7. Sandbox Analyzer-Objekte

A.7.1. Unterstützte Dateitypen und Dateiendungen für die manuelle Übermittlung

Die folgenden Dateiendungen werden unterstützt und können im Sandbox Analyzer manuell detoniert werden:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/Script, HTML (Unicode), JAR (Archiv), JS, LNK, MHTML (DOC), MHTML (PPT), MHTML (XLS), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE-Dateien (ausführbar), PDF, PEF (ausführbar), PIF (ausführbar), RTF, SCR, URL (binär), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer kann die oben genannten Dateitypen auch dann erkennen, wenn sie sich in Archiven der folgenden Typen befinden: 7z, ACE, ALZip, ARJ,

BZip2, cpio, GZip, LHA, Linux TAR, LZMA komprimiertes Archiv, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (Multivolume), ZOO, XZ.

A.7.2. Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden

Die Vorfilterung der Inhalte bestimmt Dateitypen durch eine Kombination aus Objekthalt und Dateieindung. Das bedeutet, dass eine ausführbare Datei mit der Dateieindung `.tmp` als Anwendung erkannt und bei Verdacht an den Sandbox Analyzer übermittelt wird.

- Anwendungen - Dateien im PE32-Format, einschließlich, aber nicht beschränkt auf die folgenden Dateieindungen: `exe`, `dll`, `com`.
- Dokumente - Dateien im Dokumentformat, einschließlich, aber nicht beschränkt auf die folgenden Dateieindungen: `xlsx`, `xls`, `ppt`, `doc`, `docx`, `docx`, `dot`, `chm`, `xlm`, `docm`, `dotm`, `dotm`, `potm`, `potx`, `ppam`, `ppax`, `pps`, `pps`, `ppsm`, `pptx`, `sldm`, `sldx`, `xlm`, `xltm`, `rtf`, `pdf`.
- Skripte: `ps`, `wsf`, `ws`, `php`, `py`, `js`, `vb`, `vbs`, `pyc`, `pyo`, `wsc`, `wsh`, `pssc1`, `jse`, `vbe`.
- Archive: `zip`, `jar`, `7z`, `bz`, `bz2`, `tgz`, `msi`, `rar`, `rev`, `z`, `arj`, `iso`, `lha`, `lhz`, `uu`, `uee`, `xxe`, `lzma`, `ace`, `r00`.
- E-Mails (im Dateisystem gespeichert): `eml`, `tnef`.

A.7.3. Standardausschlüsse bei automatischer Übermittlung

`asc`, `avi`, `bmp`, `gif`, `jpeg`, `jpg`, `mkv`, `mp4`, `pgp`, `png`, `txt`.

A.7.4. Empfohlene Anwendungen für die Detonations-VMs

Für die ordnungsgemäße Funktion von Sandbox Analyzer On-Premises müssen bestimmte Anwendungen auf den virtuellen Maschinen für die Detonation installiert sein, damit die übermittelten Stichproben geöffnet werden können.

Anwendungen	Dateitypen
Microsoft Office-Suite	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Reader (Zur Anzeige von PDF-Dokumenten)	pdf
Windows-Standard	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Datenprozessoren

Name	Details
Prozessoranfrageweiterleitung	Weiterleitung von Prozessoranfragen in verteilten Umgebungen
VMWare-Hypervision-Integrator	Synchronisiert das VMWare-Inventar und andere Informationen mit GravityZone
Citrix-Hypervisor-Integrator	Synchronisiert das Xen-Inventar und andere Informationen mit GravityZone

Name	Details
Generischer Virtualisierungsintegrator	Synchronisiert Nutanix-, Amazon EC2- und Azure- Inventare mit GravityZone.
NTSA-Integrator	Synchronisiert den Network Traffic Security Analytics (NTSA)-Integrationsstatus und sendet Lizenz-Updates an die NTSA-Appliance
Active-Directory-Computerinventar-Synchronisierung	Synchronisiert das Active Directory-Computerinventar mit GravityZone
Active-Directory-Gruppeninventar-Synchronisierung	Synchronisiert das Inventar der Active Directory-Gruppen mit GravityZone
Active-Directory-Benutzerimport-Synchronisierung	Synchronisiert die Active Directory-Benutzerkonten mit GravityZone (dient der Verknüpfung von AD-Konten mit GravityZone-Konten)
Active-Directory-Benutzerinventar-Synchronisierung	Synchronisiert das Active Directory-Benutzerinventar mit GravityZone
E-Mail-Verarbeitung	Stellt E-Mails zum Versand über GravityZone in eine Warteschlange
Bericht-Verarbeitung	Verarbeitet Berichte und Portlets
Windows-Sicherheitsagent-Installer	Stellt den Bitdefender-Sicherheitsagenten auf Windows-Geräten bereit
Security-Server-Installer	Stellt virtuelle Sicherheits-Appliances bereit
Lizenzmanagement	Verwaltet die Lizenzen installierter Endpunkte



Name	Details
Handy-Push-Benachrichtigungs-Verarbeitung	Sendet Push-Benachrichtigungen an geschützte Mobilgeräte
Linux- und macOS-Sicherheitsagent-Installer	Stellt den Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE)-Agenten auf Linux- und macOS-Geräten bereit
Endpunkt-Kits- und Produkt-Updater	Lädt Bitdefender-Endpunkt-Kits und -Produkt-Updates herunter und veröffentlicht sie
GravityZone-Updater	Aktualisiert GravityZone automatisch, wenn konfiguriert. Aktualisiert Versionen virtueller GravityZone-Appliances
Paketbereinigung	Bereinigt nicht verwendete Paketdateien
Sicherheitsproblem-Verarbeitung	Verarbeitet Sicherheitsprobleme für Elemente im Abschnitt Netzwerk
Backup-Verarbeitung	Führt Backups der GravityZone-Datenbank durch
Benachrichtigungs-Verarbeitung	Sendet Benachrichtigungen an Benutzer
Systemereignis-Verarbeitung	Behandelt Ereignisse aus der Infrastruktur (Anwendungssteuer, Sandbox Analyzer, Serenity, SVA) oder den Integrationen (Exchange, Nutanix, NSX)
HVI-Ergänzungspaket-Installer	Verantwortlich für die Installation, Aktualisierung und Entfernung des



Name	Details
	HVI-Ergänzungspakets für XEN-Hosts
HVI-Neustartaufgaben-Verarbeitung	Verwaltet Neustartaufgaben auf HVI-Hosts
Strom- und Online-Status-Verarbeitung	Berechnet den Stromversorgungszustand und den Verbindungsstatus von Computern und virtuellen Maschinen
Offline-Maschinen-Bereinigungs-Verarbeitung	Entfernt Offline-Maschinen aus dem Netzwerk
Hintergrundaufgabenausführung	Behandelt und führt Hintergrundaufgaben und -prozesse aus

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Boot-Sektor:

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootkit

Ein Bootkit ist ein Schadprogramm, das den Master Boot Record (MBR), den Volume Boot Record oder den Boot-Sektor infizieren kann. Ein Bootkit bleibt auch nach einem Neustart des Systems aktiv.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Andererseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Exploit

Als Exploit wird zum einen eine Methode bezeichnet, mit der Unbefugte auf einen Computer zugreifen, zum anderen eine Schwachstelle in einem System, über die das System angegriffen werden kann.

Fehlalarm

Erscheint, wenn ein Virens scanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Gezielte Angriffe

Cyber-Angriffe, die es hauptsächlich auf finanzielle Vorteile oder die Erschütterung eines guten Rufs abgesehen haben. Opfer können Einzelpersonen, Unternehmen, eine Software oder ein System sein. In jedem Fall wird das Opfer vor dem Angriff genauestens studiert. Diese Art von Angriffen wird über einen langen Zeitraum hinweg und in verschiedenen Phasen durchgeführt, wobei oft mehr als ein Einfallstor ausgenutzt wird. Sie werden kaum bemerkt, und wenn doch, dann meist erst, wenn es schon zu spät ist.

Grayware

Eine Klasse von Software-Anwendungen irgendwo zwischen legitimer Software und Malware. Sie ist zwar nicht so unmittelbar schädlich wie Malware, die die Systemfunktion direkt beeinträchtigt, ihr Verhalten ist aber dennoch beunruhigend und kann zu unerwünschten Situationen führen. Daten können gestohlen, Identitäten missbraucht und Werbung eingeblendet werden. Die verbreitetsten Arten von Grayware sind [Spyware](#) und [Adware](#).

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden

kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bössartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird. Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bössartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Scan-Ressourcenkonflikt

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet. Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.

Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Passwort-Stehler

Ein Passwort-Stehler sammelt Daten wie Benutzernamen und Passwörter für Konten. Die gestohlenen Zugangsdaten werden dann zu kriminellen Zwecken genutzt.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Ransomware

Eine Schadsoftware, die Ihren Computer sperrt oder Ihnen den Zugriff auf Ihre Dateien und Anwendungen verwehrt. Ransomware verlangt die Zahlung eines bestimmten Betrags (Lösegeldzahlung) als Gegenleistung für einen Entschlüsselungscode, der den Zugang zum Computer und Ihren Dateien wieder freigibt.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Schutzebenen

GravityZone bietet Schutz durch eine Reihe von Modulen und Rollen, die gemeinsam als Sicherheitsebenen bezeichnet werden und in Endpunktschutz (EPP) bzw. Kernschutz sowie verschiedene Add-ons unterteilt sind. Der Endpunktschutz umfasst Malware-Schutz, Advanced Threat Control, Erweiterter Exploit-Schutz, Firewall, Inhaltssteuerung, Gerätesteuerung, Network Attack Defense, Power-User und Relais. Die Add-ons umfassen Sicherheitsebenen wie Security for Exchange und Sandbox Analyzer.

Weitere Einzelheiten zu den mit Ihrer GravityZone-Lösung erhältlichen Sicherheitsebenen finden Sie unter [„GravityZone-Sicherheitsebenen“](#) (S. 2).

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht,

können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein böses Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenken. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Verdächtige Dateien und Netzwerkverkehr

Verdächtige Dateien sind solche mit einer zweifelhaften Reputation. Diese Einstufung basiert auf mehreren Faktoren, darunter: Vorhandensein der digitalen Signatur, Anzahl der Vorkommen in Computernetzwerken, verwendeter Packer, usw. Netzwerkverkehr gilt als verdächtig, wenn er vom Muster abweicht. Zum Beispiel bei unzuverlässiger Quelle, Verbindungsanfragen an ungewöhnliche Ports, hohe Bandbreitennutzung, zufällig scheinende Verbindungszeiten, usw.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, das sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegt und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Windows-Downloader

Es ist ein generischer Name für ein Programm, dessen primäre Funktion darin besteht, Inhalte zu unerwünschten oder schädlichen Zwecken herunterzuladen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.