Bitdefender

GravityZone

ADMINISTRATORHANDBUCH

Bitdefender GravityZone Administratorhandbuch

Veröffentlicht 2021.01.11

Rechtlicher Hinweis

Inhaltsverzeichnis

Vorwort

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`	Einzugebende 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. Sie bietet Sicherheitsdienste für physische Endpunkte, 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 Verhaltens-Überwachung, Schutz vor Zero-Day-Attacken, Anwendungs-Blacklists 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
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpunkt-Risikoanalyse (ERA)
- Email Security

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 bösartiger 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 Prozesstyps, 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), verschleierter 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.

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 ausgezeichneter 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. 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 Schad-Code 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.

Der Sandbox Analyzer meldet verdächtige Dateien auf den verwalteten Endpunkten automatisch, auch wenn sie von Signatur-basierten Malware-Schutz-Mechanismen nicht entdeckt werden könnten. Die Meldungen werden ausgelöst durch dedizierte Heuristiken, die im Zugriff-Malware-Schutz-Modul eingebettet sind.

Der Sandbox Analyzer verhindert, dass unbekannte Bedrohungen auf dem Endpunkt ausgeführt werden können. Er läuft entweder im Überwachungsmodus oder im Blockiermodus, in dem er den Zugriff auf verdächtige Dateien gewährt oder verweigert, bis eine Entscheidung getroffen wird. Sandbox Analyzer behandelt gefundene Bedrohungen automatisch gemäß den Bereinigungsaktionen, die in der Sicherheitsrichtilinie für die betroffenen Systeme festgelegt sind.

Außerdem können Sie mit dem Sandbox Analyzer Stichproben manuell direkt vom Control Center aus übermitteln und selbst entscheiden, wie Sie weiter mit diesen Dateien verfahren.

2.13. Endpoint Detection and Response (EDR)

Bei Endpoint Detection and Response handelt es sich um eine Komponente zur Ereigniskorrelation, mit der selbst komplexe Bedrohungen und laufende Angriffe erkannt werden können. EDR ist Bestandteil unserer umfassenden und integrierten Endpunktschutzplattform und bündelt Informationen zu Geräten aus dem gesamten Unternehmensnetzwerk. Die Lösung steht Ihren Incident-Response-Teams bei der Untersuchung und Reaktion auf komplexe Bedrohungen helfend zur Seite.

Mit Bitdefender Endpoint Security Tools können Sie das Sicherheitsmodul EDR Sensor auf Ihren verwalteten Endpunkten aktivieren, um Hardware- und Betriebssystemdaten zu sammeln. Aufbauend auf einem Client/Server-Framework werden die Metadaten auf beiden Seiten erfasst und verarbeitet.

Mit dieser Komponente erhalten Sie detaillierte Informationen zu gefundenen Vorfällen, ein interaktives Vorfallsdiagramm, Bereinigungsaktionen und die Integration mit dem Sandbox Analyzer sowie HyperDetect.

2.14. Endpunkt-Risikoanalyse (ERA)

Endpoint Risk Analytics (ERA) identifiziert, bewertet und behebt Windows Endpunkt-Schwachstellen durch Sicherheitsrisiko-Scans (Bei Bedarf oder per Richtlinie avisiert), durch die Überprüfung einer grossen Anzahl an Risiko-Indikatoren. Nachdem Sie Ihr Netzwerk auf bestimmte Risikoindikatoren gescannt haben, erhalten Sie eine Übersicht zu Ihrem Netzwerk-Risiko-Status im **Risiko-Management**-Dashboard im Hauptmenü. Im GravityZone Control Center können Sie bestimmte Sicherheitsrisiken automatisch beheben und Empfehlungen zur Risikominimierung auf den Endpunkten einsehen.

2.15. Email Security

Mit Email Security können Sie die E-Mail-Zustellung steuern, Nachrichten filtern und unternehmensweite Richtlinien anwenden, um gezielte Angriffe und Betrugsmaschen wie E-Mail-Adressenimitation (BEC) oder „CEO Fraud“ abzuwehren. Für den Zugriff auf die Konsole erfordert Email Security Account Provisioning. Weitere Informationen hierzu finden Sie im Benutzerhandbuch für Bitdefender Email Security.

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. 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

GravityZone besteht aus den folgenden Komponenten:

- Web-Konsole (Control Center)
- Security Server
- Sicherheitsagenten

3.1. Web-Konsole (GravityZone Control Center)

Bitdefender-Sicherheitslösungen werden innerhalb der GravityZone von einer zentralen Stelle aus verwaltet: dem Control Center. Diese Web-Konsole erleichtert die Verwaltung, indem sie einen Überblick über die gesamte Sicherheitslage des Unternehmens bietet und die Steuerung aller Sicherheitsmodule für virtuelle und physische Arbeitsplatzrechner und Server sowie für Amazon-Instanzen ermöglicht. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst größter Unternehmen zu erfüllen.

Das Control Center, eine Web-basierte Oberfläche, lässt sich in bestehende System-Management- und Überwachungssystemen integrieren und erleichtert so den Schutz nicht-verwalteter Arbeitsplatzrechner und Server.

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.

Security Server muss auf genügend Hosts installiert sein, um die gewünschte Anzahl an virtuellen Maschinen gewährleisten zu können.

3.3. 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

3.3.1. 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
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpunkt-Risikoanalyse (ERA)

Endpunktrollen

- 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.

  Diese Funktion ist für die sichere Agenteninstallation in einer GravityZone-Cloud-Umgebung unabdingbar.
- 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 Zielendpunkten 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.

3.3.2. 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. Sandbox Analyzer-Architektur

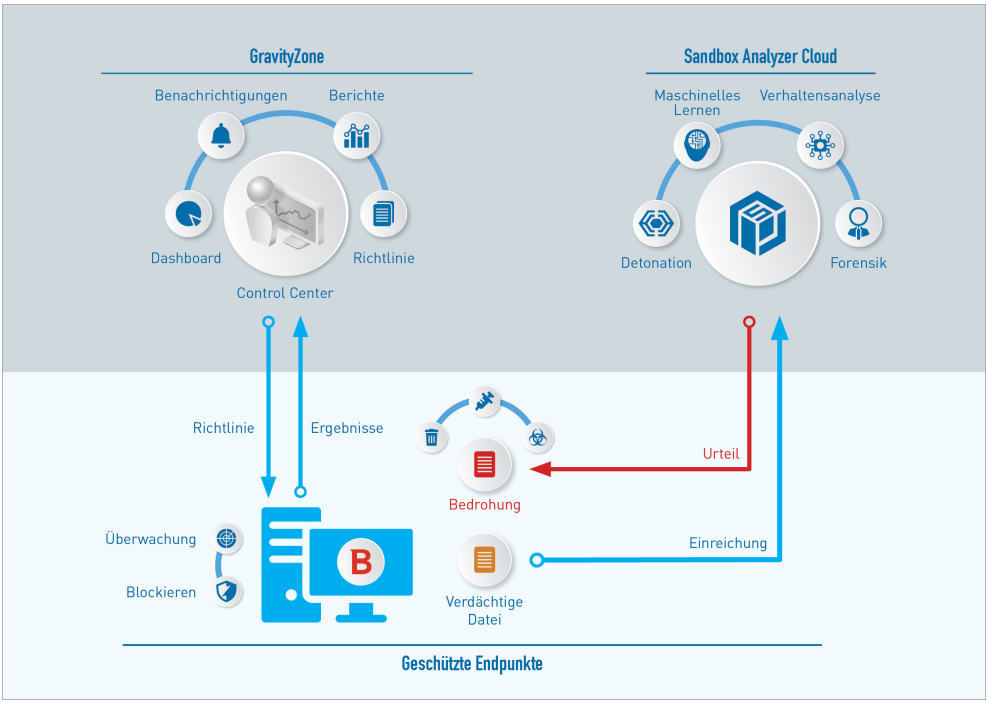
Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben.

Der Sandbox Analyzer umfasst die folgenden Komponenten:

- **Sandbox Analyzer-Portal**. Bei dieser Komponente handelt es sich um einen gehosteten Kommunikationsserver, der Anfragen zwischen Endpunkten und dem Bitdefender-Sandbox-Cluster bearbeitet.
- **Sandbox Analyzer-Cluster**. Bei dieser Komponente handelt es sich die gehostete Sandbox-Infrastruktur, innerhalb derer die virtuelle Verhaltensanalyse vorgenommen wird. 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-Architektur

Sobald der Sandbox Analyzer-Dienst über das Control Center aktiviert wurde, passiert Folgendes:

1. Der Bitdefender-Sicherheitsagent beginnt, verdächtige Dateien, die mit den Sicherheitsregeln in der Richtlinie übereinstimmen, zu melden.
2. Nach der Analyse der Dateien wird eine Antwort ans Portal und dann weiter an den Endpunkt geleitet.
3. Wenn eine Datei als gefährlich erkannt wird, wird der Benutzer benachrichtigt und eine Bereinigungsaktion ausgeführt.

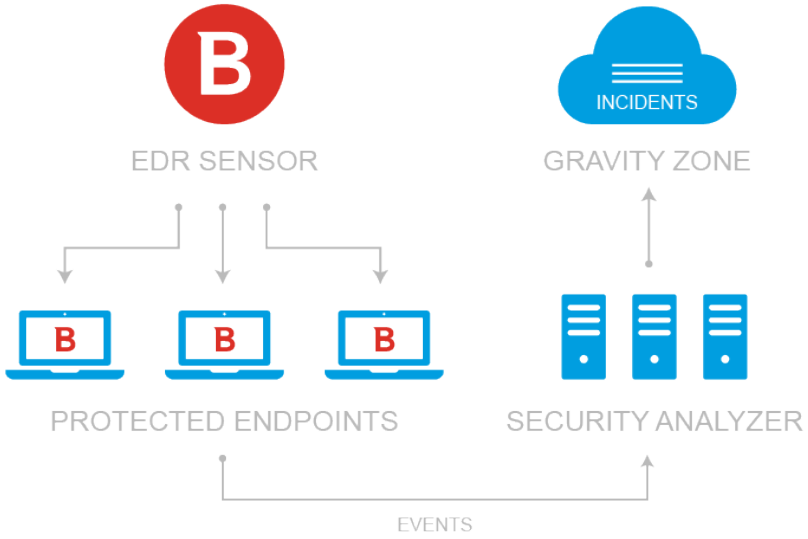
Die Analyseergebnisse werden mit ihrem Datei-Hash-Wert in der Sandbox Analyzer-Datenbank gespeichert. Wenn eine bereits zuvor analysierte Datei von einem anderen Endpunkt gemeldet wird, wird sofort eine Antwort zurückgegeben, da die Ergebnisse bereits in der Datenbank vorhanden sind.

3.5. EDR-Architektur

Zur Erkennung von komplexen Bedrohungen und laufenden Angriffen benötigt EDR Hardware- und Betriebssystemdaten. Einige der Rohdaten werden lokal verarbeitet, während maschinelle Lernalgorithmen in den Security Analytics komplexere Aufgaben übernehmen.

EDR umfasst zwei Hauptkomponenten:

- Den Vorfall-Sensor, der Daten zu Prozessen, Endpunkten und zum Verhalten von Anwendungen erfasst und entsprechende Berichte erstellt.
- Die Security Analytics, eine Backend-Komponente der Bitdefender-Suite, mit der die vom Vorfall-Sensor erhobenen Metadaten ausgewertet werden.



EDR im Zusammenhang mit Datenfluss vom Endpunkt zum Control Center

4. ERSTE SCHRITTE

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. Öffnen Sie Ihren Internet-Browser.
2. Rufen Sie die folgende Seite auf: https://gravityzone.bitdefender.com
3. Bei der Anmeldung mit **GravityZone-Zugangsdaten**:
   a. Geben Sie die E-Mail-Adresse Ihres Kontos ein und klicken Sie auf **Weiter**.
   b. Geben Sie das Passwort für Ihr Konto ein und klicken Sie dann auf **Weiter**.
   c. Geben Sie als Bestandteil der Zwei-Faktor-Authentifizierung den sechsstelligen Code aus der Authentifizierungsanwendung ein.
   d. Klicken Sie zur Anmeldung auf **Fortfahren**.

   Bei der Anmeldung mit **Single Sign-On (SSO)**:
   a. Geben Sie bei der ersten Anmeldung die E-Mail-Adresse Ihres Kontos ein und klicken Sie auf **Weiter**.

      Sie werden dann von GravityZone zur Authentisierungsseite Ihres Identitätsanbieters weitergeleitet.
   b. Authentisieren Sie sich bei Ihrem Identitätsanbieter.
   c. Vom Identitätsanbieter werden Sie dann zurück zu GravityZone geleitet, wo Sie automatisch am Control Center angemeldet werden.

Beim nächsten Mal können Sie sich am Control Center einfach nur mit Ihrer E-Mail-Adresse anmelden.

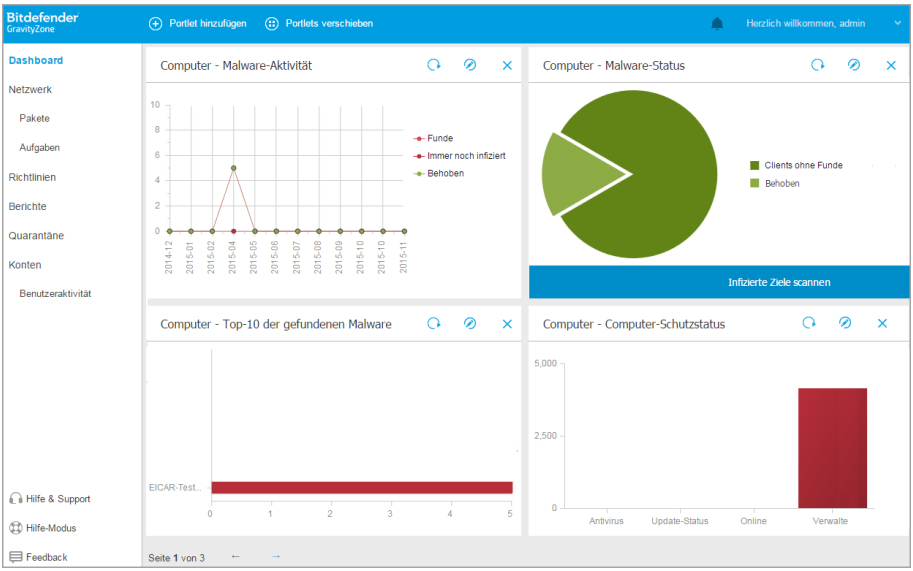
Bei der ersten Anmeldung müssen Sie den Bitdefender-Nutzungsbedingungen zustimmen. Mit einem Klick auf **Fortfahren** können Sie mit der Nutzung von GravityZone loslegen.

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.
- Sollte Sie GravityZone bei der Anmeldung mit SSO nach einem Passwort fragen, wenden Sie sich bitte an Ihren Administrator. In der Zwischenzeit können Sie sich mit Ihrem vorigen Passwort anmelden oder über den Link zur Passwortwiederherstellung ein neues Passwort anfordern.

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

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.

Vorfälle
Sicherheitsvorfälle aus dem gesamten Unternehmensnetzwerk anzeigen und verwalten.

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 die Einstellungen für Control Center Netzwerkinventar, einschließlich geplanter Regeln für die automatische Bereinigung nicht verwendeter virtueller Maschinen.

> **Beachten Sie**
> Dieses Menü steht nur Benutzern zur Verfügung, die die Berechtigung **Netzwerke verwalten** haben.

Links unten im Control Center im Bereich **Extras** stehen noch weitere GravityZone-Funktionen zur Verfügung, z. B. die manuelle Dateiübermittlung an den Sandbox Analyzer.

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.
- **Mein Unternehmen**. Klicken Sie auf diese Option, um Ihre Unternehmenskontoinformationen und -einstellungen zu verwalten.
- **Zugangsdaten-Manager**. Klicken Sie auf diese Option, um die für Ferninstallationsaufgaben nötigen Authentifizierungsdaten hinzuzufügen und zu verwalten.

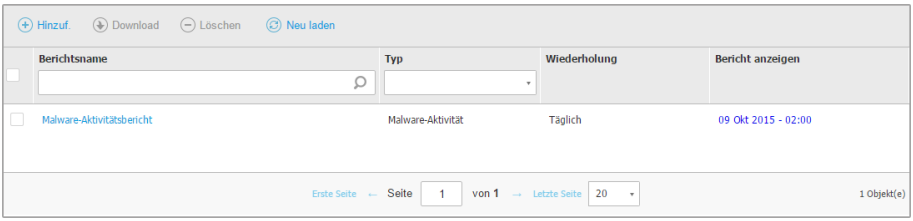
- **Hilfe & Support**. Klicken Sie auf diese Option, um Hilfe- und Support-Informationen zu erhalten.
- **Feedback**. Klicken Sie auf diese Option, um ein Formular zu öffnen, über das Sie uns Rückmeldung zu Ihren Erfahrungen mit GravityZone geben können.
- **Abmelden**. Klicken Sie auf diese Option, 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.



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

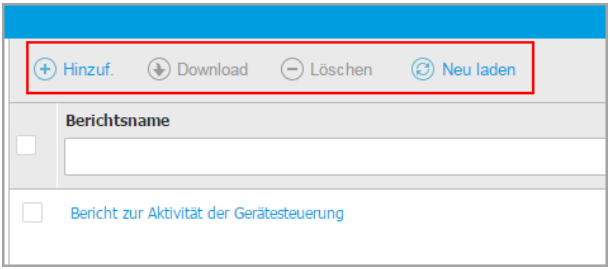
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**.

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:

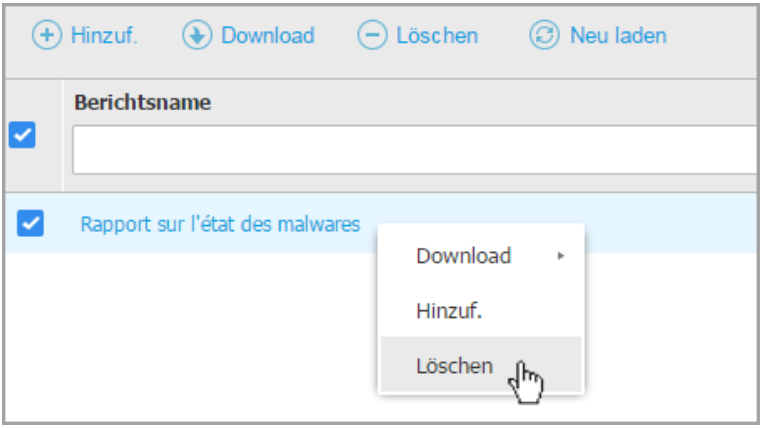
- Neuen Bericht erstellen.
- Einen geplanten Bericht herunterladen.
- Einen geplanten Bericht löschen.



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.

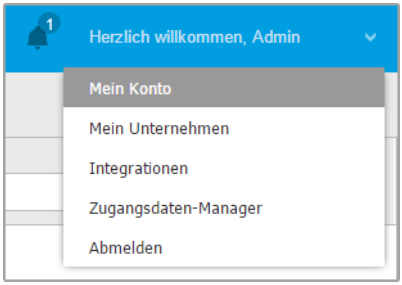


Die Berichteseite - Kontextmenü

4.3. 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**.
   - **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-Authentifzierung.** 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.

Es empfiehlt sich, wie folgt vorzugehen:

- 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.

4.5. Ihr Unternehmen verwalten

Als Benutzer mit der Rolle **Eigenes Unternehmen verwalten**können Sie Ihre Unternehmensdetails und Lizenzeinstellungen einsehen und ändern und

Authentifizierungseinstellungen verwalten, so z. B. Zwei-Faktor-Authentifizierung und Single Sign-On.

4.5.1. Details und Lizenzeinstellungen

So überprüfen oder ändern Sie Details Ihres Unternehmens und Lizenz-Einstellungen:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
2. Geben Sie im Bereich **Unternehmensdetails** Informationen wie den Namen, die Adresse und die Telefonnummer Ihres Unternehmens ein.

   So können Sie das Logo, das im Control Center und in den Berichten und E-Mails Ihres Unternehmens angezeigt wird, ändern:

   - Klicken Sie auf **Ändern**, um das Logobild auf Ihrem Computer zu suchen. Das Dateiformat muss entweder PNG oder JPG sein, und das Bild muss genau 200×30 Pixel groß sein.
   - Klicken Sie auf **Standard**, um das Bild zu löschen und wieder das von Bitdefender bereitgestellte Bild zu verwenden.
3. Ihr Unternehmen kann standardmäßig über die Partnerkonten anderer Unternehmen verwaltet werden, die Ihr Unternehmen vielleicht in ihrer Bitdefender Control Center gelistet haben Sie können den Zugriff dieser Unternehmen auf Ihr Netzwerk blockieren, indem Sie die Option **Partnern erlauben, bei der Verwaltung der Sicherheit dieses Unternehmens zu helfen** deaktivieren. Danach wird Ihr Netzwerk nicht im Control Center anderer Unternehmen angezeigt, diese können Ihr Abonnement aber noch verwalten.
4. Im Bereich **Lizenz** können Sie Ihre Lizenzdetails einsehen und bearbeiten sowie einen Add-on-Schlüssel eingeben.
   - So fügen Sie einen neuen Lizenzschlüssel hinzu:
     a. Wählen Sie im Menü **Typ** den Abonnementtyp **Lizenz** aus.
     b. Geben Sie im Feld **Lizenzschlüssel** den Lizenzschlüssel ein.
     c. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
   - Unter dem Lizenzschlüssel werden Informationen zu diesem Lizenzschlüssel angezeigt:

- **Ablaufdatum**: das Datum, bis zu dem der Lizenzschlüssel verwendet werden kann.
- **Benutzt**: die Anzahl der benutzten Lizenzplätze im Verhältnis zur Anzahl der insgesamt im Lizenzschlüssel enthaltenen. Ein Lizenzplatz gilt als benutzt, wenn der Bitdefender-Client auf einem Endpunkt in dem von Ihnen verwalteten Netzwerk installiert wurde.
- **Gesamt**: die Gesamtzahl der Lizenzplätze Ihrer Lizenz bzw. Ihres Abonnements.

Falls Sie darüber hinaus über ein Monatsabonnement verfügen, können Sie in **Monatslizenznutzung** einen Bericht über den laufenden Monat generieren. Weitere Informationen finden Sie unter Monatslizenznutzung .

- So geben Sie einen Add-on-Schlüssel ein:
  - Geben Sie den Schlüssel ins Feld **Add-on-Schlüssel** ein.
  - Klicken Sie auf **Hinzufügen** und warten Sie, bis GravityZone den Add-on-Schlüssel geprüft hat. Wenn er gültig ist, ruft das Control Center die folgenden Informationen zum Add-on ab: den Typ, den Schlüssel und die Option, es zu entfernen.

> **Beachten Sie**
> Wenn Sie eine Test- oder Monatslizenz haben, wird das Feld **Add-on-Schlüssel** nicht angezeigt.

5. Unter **Bitdefender Partner** finden Sie Informationen zu Ihrem Dienstleister.

   So wechseln Sie Ihren Managed-Service-Anbieter:

   a. Klicken Sie auf die Schaltfläche **Ändern**.

   b. Geben Sie die Kennung des Partnerunternehmens im Feld **Partnerkennung** ein.

> **Beachten Sie**
> Unternehmen können ihre Kennung auf der Seite **Mein Unternehmen** einsehen. Wenn Sie eine Vereinbarung mit einem Partnerunternehmen getroffen haben, muss ein Unternehmensvertreter Ihnen die Control-Center-Kennung des Unternehmens mitteilen.

   c. Klicken Sie auf **Speichern**.

Ihr Unternehmen wird so automatisch aus der Control Center des alten Partners in die des neuen Partners verschoben.

6. Wenn Sie möchten, können Sie über die entsprechenden Felder Ihr Unternehmen mit Ihrem MyBitdefender-Konto verknüpfen.
7. Klicken Sie **Speichern**, um die Änderungen zu speichern.

4.5.2. Authentisierungseinstellungen

GravityZone bietet zusätzliche Optionen zur sicheren Benutzerauthentifizierung im Control Center, so z. B.:

- Zwei-Faktor-Authentifzierung
- Passwortablauf
- Kontosperre
- Single Sign-on

Als Unternehmensadministrator können Sie diese zusätzlichen Sicherheitsmaßnahmen für die Anmeldung bequem für Ihr gesamtes Unternehmen aktivieren:

1. Rufen Sie die Seite **Konfiguration > Authentisierungseinstellungen** auf.
2. Wählen oder konfigurieren Sie die Optionen, die Sie aktivieren müssen.

   Weitere Einzelheiten zu jeder Option finden Sie in den folgenden Abschnitten.
3. Klicken Sie auf **Speichern**, um sie anzuwenden.

Zwei-Faktor-Authentifizierung erzwingen

Zwei-Faktor-Authentifizierung (2FA) gewährleistet, dass die Person, die versucht, sich beim Control Center anzumelden, der vorgesehene Benutzer ist. 2FA fordert bei jeder Anmeldung zusätzlich zu den Anmeldeinformationen für das Control Center einen Authentifizierungscode an. GravityZone nutzt die Google Authenticator-App für die Generierung des 2FA-Authentifizierungscodes.

In GravityZone ist die Erzwingung der Zwei-Faktor-Authentifizierung standardmäßig für das gesamte Unternehmen aktiviert. Das bedeutet, dass alle GravityZone-Benutzer 2FA konfigurieren und mit ihren Benutzerkonten verwenden müssen.

Wenn Sie die Markierung für diese Option aufheben, wird die 2FA-Erzwingung deaktiviert. Sie müssen diese Aktion bestätigen. Das bewirkt, dass 2FA auch weiterhin für die Benutzer aktiviert bleibt, diese sie aber in ihren Kontoeinstellungen deaktivieren können.

Beachten Sie

- Den 2FA-Status für ein Benutzerkonto können Sie auf der **Konten**seite einsehen.
- Wenn sich ein Benutzer mit aktivierter 2FA-Authentifizierung nicht bei GravityZone anmelden kann (aufgrund eines neuen Geräts oder verlorenen geheimen Schlüssels für Google Authenticator), können Sie die Aktivierung der Zwei-Faktor-Authentifizierung in seinen Kontoeinstellungen auf der Seite **Konten** zurücksetzen. Weitere Informationen finden Sie unter „Zwei-Faktor-Authentifizierung verwalten“ (S. 41).

Höchstalter für Passwörter auf 90 Tage setzen

Mit dieser Option wird die Kontoablaufrichtlinie aktiviert. Benutzer müssen ihr Passwort vor Ablauf dieses Zeitraums ändern. Andernfalls können sie sich nicht mehr bei GravityZone anmelden.

Konten nach 5 Anmeldeversuchen mit falschem Passwort sperren

Mit dieser Option können Sie die Anzahl der aufeinander folgenden Anmeldeversuche mit falschem Passwort beschränken, um Missbrauch zu verhindern. Wenn die festgelegte Höchstzahl an Fehlversuchen erreicht ist, wird das Konto gesperrt und der Benutzer muss ein neues Passwort festlegen.

Die Richtlinie gilt für die in GravityZone erstellten Konten.

Single Sign-on mit SAML konfigurieren

GravityZone unterstützt vom Dienstanbieter initiiertes Single Sign-On (SSO) als eine einfache und sichere Alternative zur klassischen Anmeldung mit Benutzername und Passwort.

Diese Methode erfordert die Integration mit Identitätsanbietern von Drittanbietern (IdP), die SAML 2.0 verwenden, wie AD FS, Okta und Azure AD, die GravityZone-Benutzer authentifizieren und ihnen den Zugriff auf das Control Center ermöglichen.

So funktioniert GravityZone SSO:

1. Benutzer geben ihre E-Mail-Adressen auf der GravityZone-Anmeldeseite ein.

2. GravityZone erstellt eine SAML-Anforderung und leitet die Anforderung und die Benutzer an den Identitätsanbieter weiter.
3. Die Benutzer müssen sich bei dem Identitätsanbieter authentifizieren.
4. Nach der Authentifizierung sendet der Identitätsanbieter eine Antwort an GravityZone in Form eines mit einem X.509-Zertifikat signierten XML-Dokuments. Außerdem leitet der Identitätsanbieter die Benutzer zu GravityZone um.
5. GravityZone ruft die Antwort ab, validiert sie mit dem Fingerabdruck des Zertifikats und ermöglicht es den Benutzern, sich ohne weitere Interaktion beim Control Center anzumelden.

Benutzer melden sich so lange automatisch beim Control Center an, wie sie eine aktive Sitzung mit dem Identitätsanbieter haben.

Um SSO zu aktivieren, müssen Sie Folgendes tun:

1. Konfigurieren Sie den Identitätsanbieter so, dass GravityZone als Dienstanbieter verwendet wird. Informationen zu unterstützten Identitätsanbietern und Konfigurationsdetails finden Sie in diesem Artikel in der Wissensdatenbank.
2. Aktivieren Sie SSO für Ihr Unternehmen:
   a. Geben Sie unter **Single Sign-on mit SAML konfigurieren** die Metadaten-URL des Identitätsanbieters in das entsprechende Eingabefeld ein und klicken Sie auf **Speichern**.
   b. Klicken Sie auf **Speichern**.
3. Konfigurieren Sie die Benutzer Ihres Unternehmens so, dass sie sich bei ihrem Identitätsanbieter authentifizieren. Weitere Einzelheiten dazu finden Sie unter „Authentisierungsmethoden verwalten“ (S. 39).

Wichtig
Als GravityZone-Administrator können Sie Single Sign-On für Benutzer Ihres Unternehmens konfigurieren, jedoch aus Sicherheitsgründen nicht für Ihr eigenes Konto.

So deaktivieren Sie Single Sign-on für Ihr Unternehmen:

1. Löschen Sie die Metadaten-URL des Identitätsanbieters.
2. Klicken Sie auf **Speichern** und bestätigen Sie die Aktion.

Wenn Sie Single Sign-on für Ihr Unternehmen deaktivieren, müssen sich die Benutzer wieder mit den GravityZone-Zugangsdaten anmelden. Diese Umstellung erfolgt

automatisch. Benutzer können ein neues Passwort anfordern, indem Sie auf der Anmeldeseite des Control Center auf den Link **Passwort vergessen?** klicken und den Anweisungen folgen.

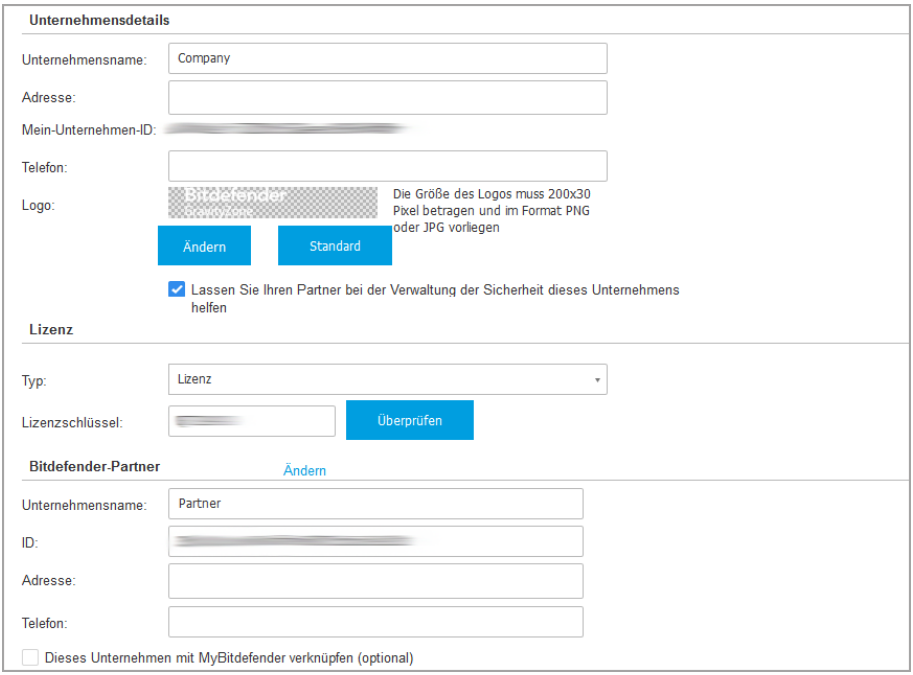
Wenn Sie zu einem späteren Zeitpunkt SSO für Ihr Unternehmen wieder aktivieren, werden sich die Benutzer zunächst weiterhin mit den GravityZone-Zugangsdaten am Control Center anmelden. Sie müssen jedes Konto einzeln manuell für die Anmeldung mit SSO konfigurieren.

5. BENUTZERKONTEN

Mit dem Konto, das Sie bei Abschluss des Abonnements erstellt haben, können Sie dann GravityZone über das Control Center einrichten und verwalten.

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

- Sie können interne Benutzerkonten anlegen, um anderen Mitarbeitern im Unternehmen Zugriff auf die Control Center zu ermöglichen. 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.



Die Kontenübersicht

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

- Benutzername des Kontos.
- E-Mail-Adresse des Kontos (die zur Anmeldung am Control Center verwendet wird). 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)
- Der Status der Zwei-Faktor-Authentifizierung (2FA). Hier können Sie überprüfen, ob der Benutzer die Zwei-Faktor-Authentifizierung aktiviert hat.

- Authentisierungsmethode, worunter angegeben ist, ob sich der Benutzer mit den GravityZone-Zugangsdaten oder mittels Single Sign-on (SSO) über einen Identitätsanbieter anmeldet.

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** - Geeignet für Manager von Kundenunternehmen, die eine GravityZone-Lizenz von einem Partner erworben haben. Ein Unternehmensadministrator verwaltet die Lizenz, das Unternehmensprofil und die gesamte GravityZone-Installation. Er erhält somit umfassende Kontrolle über alle Sicherheitseinstellungen (es sei denn, dies wurde im Rahmen eines Dienstleisterszenarios von dem übergeordneten Partnerkonto außer Kraft gesetzt). Unternehmensadministratoren können ihre Aufgaben mit untergeordneten Administrator- und Sicherheitsanalystenkonten 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** - Sicherheitsanalystenkonten 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 im Kapitel „Benutzerrechte“ (S. 36).

Rolle des Kontos	Zugelassene untergeordnete Konten	Benutzerrechte
Unternehmensadministrator	Unternehmensadministratoren, Netzwerkadministratoren, Sicherheitsanalysten	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:

- **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

Bevor Sie ein Benutzerkonto anlegen, sollten Sie sicherstellen, dass Sie die benötigte E-Mail-Adresse zur Hand haben. Diese Adresse wird zwingend für das Anlegen des GravityZone-Benutzerkontos benötigt. Benutzern werden die GravityZone-Zugangsdaten an die angegebene E-Mail-Adresse gesendet.

5.3.1. Einzelverwaltung von Benutzerkonten

Im Control Center können Sie Benutzerkonten einzeln erstellen, bearbeiten und 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:
   - – **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.

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.
   - **Authentisierungsmethode**. Diese Einstellung steht für Konten unter einem Unternehmen mit aktiviertem SSO zur Verfügung. Wählen Sie aus dem Menü entweder die Anmeldung über die GravityZone-Zugangsdaten oder über einen Identitätsanbieter. Näheres zu den verfügbaren Authentisierungsmethoden erfahren Sie unter „Authentisierungsmethoden verwalten“ (S. 39).
   - **Rolle**. Wählen Sie die Rolle des Benutzers aus. Weitere Details zu Benutzerrollen finden Sie unter „Benutzerrollen“ (S. 35).
   - **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. 36).
   - **Ziele wählen**. Wählen Sie die Netzwerkgruppen aus, auf die der Benutzer Zugriff haben wird.
5. Klicken Sie auf **Speichern**, um den Benutzer hinzuzufügen. Das neue Konto erscheint in der Liste der Benutzerkonten.

> **Beachten Sie**
> Das Passwort für jedes Benutzerkonto wird automatisch nach Anlegen des Kontos vergeben und gemeinsam mit den anderen Kontodaten an die E-Mail-Adresse des Benutzers gesendet.
> Sie können das Passwort nach Anlegen des Kontos ändern. Klicken Sie in der **Konten**-Übersicht auf den Kontonamen, um das Passwort zu bearbeiten. Benutzer werden per E-Mail umgehend über die Änderung des Passworts informiert.
> Benutzer können ihr Anmeldepasswort über die Control Center ändern, indem Sie die Seite **Mein Konto** aufrufen.

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**.

5.4. Authentisierungsmethoden verwalten

Wenn Sie ein Benutzerkonto unter einem Unternehmen mit aktiviertem Single Sign-On (SSO) erstellen oder bearbeiten, können Sie konfigurieren, wie die Anmeldung beim Control Center erfolgt.

Im Bereich **Einstellungen und Rechte** finden Sie die folgenden Optionen:

- **Anmeldung mit GravityZone-Zugangsdaten**. Wenn diese Option ausgewählt wird, erfolgt die Anmeldung am Control Center mit Benutzername und Passwort.
- **Anmeldung über den Identitätsanbieter**. Wählen Sie diese Option für dieses Konto, um Single Sign-On (SSO) zu verwenden.

Sie können die Authentifizierungsmethode für jedes GravityZone-Benutzerkonto einzeln konfigurieren.

GravityZone unterstützt verschiedene Authentifizierungsmethoden für Benutzer desselben Unternehmens. Folglich ist es möglich, dass sich einige Konten mit

Benutzername und Passwort anmelden, während sich andere über einen Identitätsanbieter authentifizieren.

Näheres zur Aktivierung von SSO für Ihr Unternehmen erfahren Sie unter „Single Sign-on mit SAML konfigurieren“ (S. 30).

Wichtig

- Als GravityZone-Administrator können Sie Single Sign-On für Benutzer Ihres Unternehmens konfigurieren, jedoch aus Sicherheitsgründen nicht für Ihr eigenes Konto.
- Für SSO müssen Benutzer für GravityZone die gleiche E-Mail-Adresse wie beim Identitätsanbieter verwenden. GravityZone SSO unterscheidet bei E-Mail-Adressen zwischen Groß- und Kleinschreibung. So unterscheidet sich **username@company.domain** z. B. von **UserName@company.domain** und **USERNAME@company.domain**.
- Bitdefender betreibt zwei GravityZone-Cloud-Instanzen. In einigen Fällen müssen die Benutzer bei der ersten Anmeldung eine der Instanzen auswählen.

Die Änderungen an den SSO-Einstellungen für GravityZone-Benutzer können Sie auf der Seite **Konten > Benutzeraktivität** einsehen, wenn Sie die Aktivitätsprotokolle dort nach Bereich > Authentisierungseinstellungen filtern.

5.5. 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.

5.6. 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
Wenn Sie über ein Unternehmensadministrator-Benutzerkonto verfügen, können Sie die Zwei-Faktor-Authentifizierung für alle GravityZone-Benutzerkonten in Ihrem Unternehmen zwingend erforderlich machen. Weitere Informationen finden Sie im Kapitel „Ihr Unternehmen verwalten“ (S. 26).

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.

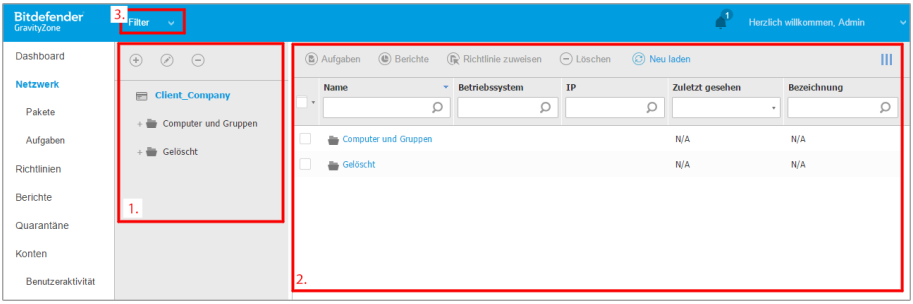
Es ist auch möglich, 2FA-Änderungen im Zusammenhang mit den Benutzerkonten nachzuverfolgen, indem Sie die Seite **Konten > Benutzeraktivität** aufrufen und die folgenden Filter auf die Aktivitätsprotokolle anwenden:

- Bereich > Konten / Unternehmen
- Aktion > Änderung

Weitere Informationen zur Aktivierung von 2FA finden Sie unter„Verwalten Ihres Kontos“ (S. 23)

6. ENDPUNKTE VERWALTEN

Auf der Seite **Netzwerk** finden sich viele Funktionen zum Durchsuchen und Verwalten der verfügbaren Endpunkte. Die **Netzwerk**-Seite besteht aus einer Oberfläche mit zwei Fenstern, in denen der Status aller Endpunkte in Echtzeit angezeigt wird:



Die Netzwerk-Übersicht

1. Im linken Fenster werden die verfügbaren Netzwerke in Baumansicht angezeigt.

   Alle gelöschten Endpunkte sind im Ordner **Gelöscht** gespeichert. Weitere Informationen finden Sie unter „Endpunkte aus dem Netzwerkinventar löschen“ (S. 118).

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

2. Im rechten Fenster wird der Inhalt der Gruppe, die Sie im Netzwerkbaum ausgewählt haben, angezeigt. 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. 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. 482).

- 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. Über das **Filter**-Menü oben im Netzwerkfenster können Sie mithilfe verschiedener Filterkriterien die Anzeige auf bestimmte Netzwerkobjekte beschränken.

Auf der **Netzwerk**-Seite können Sie auch die Installationspakete und Aufgaben für Ihre Endpunkte verwalten.

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

Um die Endpunkte anzuzeigen, die zu Ihrem Konto gehören, öffnen Sie die Seite **Netzwerk** und wählen Sie die gewünschte Netzwerkgruppe im linken Fenster aus.

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 Endpunktdetails an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **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.

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

- Den Status des Endpunkts überprüfen
- Endpunktdetails anzeigen
- Endpunkte in Gruppen organisieren.

- Sortieren, filtern und suchen
- Patches verwalten
- Aufgaben ausführen
- Definition der Active-Directory-Integration
- Schnellberichte erstellen
- Regeln zuweisen
- Endpunkte aus dem Netzwerkinventar löschen

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.

6.1. Status der Endpunkts überprüfen

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

Unter „Netzwerkobjekttypen und -status“ (S. 482) finden Sie eine Liste aller Symbole und Status.

Detaillierte Statusinformationen finden Sie unter:

- Verwaltungsstatus
- Verbindungsstatus
- Sicherheitsstatus

6.1.1. Verwaltungsstatus

Endpunkte haben immer einen der folgenden Verwaltungsstatus:

- **Verwaltet** - Endpunkte, auf denen der Sicherheitsagent installiert ist.
- **Neustart steht aus** - Endpunkte, die nach Installation oder Aktualisierung von Bitdefender einen Systemneustart erfordern.
- **Nicht verwaltet** - gefundene Endpunkte, auf denen der Sicherheitsagent noch nicht installiert wurde.
- **Gelöscht** - Endpunkte, die Sie aus dem Control Center gelöscht haben. Weitere Informationen finden Sie im Kapitel „Endpunkte aus dem Netzwerkinventar löschen“ (S. 118).

6.1.2. Verbindungsstatus

Der Verbindungsstatus betrifft alle virtuellen Maschinen und nur die verwalteten Computer. Verwaltete Endpunkte können einen der folgenden Status haben:

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

Ein Endpunkt gilt als offline, wenn der Sicherheitsagent länger als 5 Minuten inaktiv ist. Mögliche Gründe, weshalb Endpunkte als offline angezeigt werden:

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

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

- Der Sicherheitsagent hat keine Verbindung zum Bitdefender Control Center oder zum zugewiesenen Endpoint Security Relay:
  - Die Verbindung des Endpunkts 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.
  - Der Endpunkt befindet sich hinter einem Proxy-Server, und in der zugewiesenen Richtlinie wurden die Proxy-Einstellungen nicht korrekt konfiguriert.

    Warnung
    Bei Endpunkten hinter einem Proxy-Server müssen die Proxy-Einstellungen im Installationspaket des Sicherheitsagenten korrekt konfiguriert sein, da der Endpunkt 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 vom Endpunkt deinstalliert, während der Endpunkt 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 einem Endpunkt benachrichtigt und der Endpunkt wird als nicht verwaltet gekennzeichnet.

- Der Sicherheitsagent funktioniert unter Umständen nicht richtig.

So finden Sie heraus, wie lange Endpunkte inaktiv waren:

1. Zeigen Sie nur die verwalteten Endpunkte 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 Endpunkte nach dem Zeitraum ihrer Inaktivität zu sortieren.

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

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

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

6.1.3. Sicherheitsstatus

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

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

Ein Endpunkt 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:
  - 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 Endpunkt 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 Informationsseite 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. Endpunktdetails anzeigen

Gehen Sie folgendermaßen vor, um Details zu den einzelnen Endpunkten auf der **Netzwerk**seite abzurufen:

- Aufrufen der **Netzwerk**seite
- Aufrufen des **Information**sfensters

6.2.1. Aufrufen der Netzwerkseite

Detailinformationen zu einem Endpunkt finden Sie auf der **Netzwerk**seite 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 die gewünschte Gruppe aus dem linken Fenster.

   Alle Endpunkte der gewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Der Status eines Endpunktes ist durch ein Symbol klar gekennzeichnet. Detaillierte Informationen finden Sie im Kapitel „Status der Endpunkts überprüfen“ (S. 45).

4. Die einzelnen Spalten enthalten verschiedene Informationen zu jedem Endpunkt.

   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 **Information**sfenster 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.

6.2.2. Aufrufen des Informationsfensters

Klicken auf der **Netzwerk**seite im Fenster rechts auf den Namen des Endpunktes, den Sie im **Information**sfenster 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“

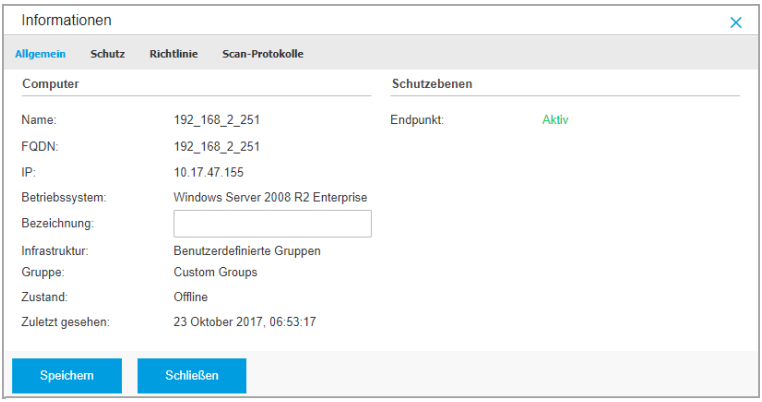
- Allgemeine Informationen zum Endpunkt wie Name, FQDN-Informationen, IP-Adresse, Betriebssystem, Infrastruktur, übergeordnete Gruppe und aktueller Verbindungsstatus.

  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 Endpunktfiltern finden Sie im Kapitel „Sortieren, Filtern und Suchen von Endpunkten“ (S. 65).

- 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.
- Für Endpunkte mit der Active-Directory-Integrator-Rolle: Der Domainname und das Datum und der Zeitpunkt der letzten Synchronisation.



Fenster Informationen - Reiter Allgemein

Reiter Schutz

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

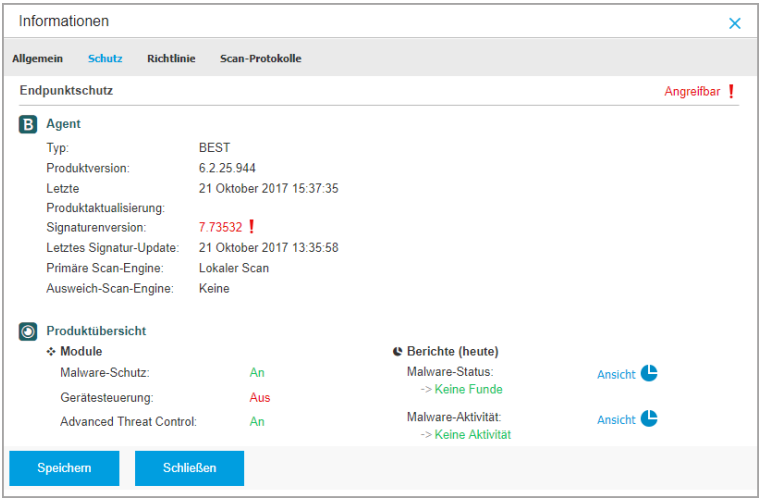
- Informationen zum Sicherheitsagenten wie Produktname, Version, Update-Status und Update-Adressen sowie die Konfiguration der Scan-Engines und Versionen der Sicherheitsinhalte. Im Falle vom Exchange-Schutz ist auch die Version der Spam-Schutz-Engine verfügbar.
- Sicherheitsstatus für jede Schutzebene. 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. 47).
- 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 Berichtoptionen anzuzeigen und den Bericht anzulegen. Weitere Informationen finden Sie unter „Berichte erstellen“ (S. 428)
- 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. 117).

- Informationen zu den Security Analytics als EDR-Bestandteil:
  - Agentenspezifische Informationen zeigen:
    - Ereignisanbieter - BEST meldet Endpunkt- und Anwendungsverhalten an die Security-Analytics-Komponente.
    - Kommunikationsstatus - BEST stellt eine Verbindung mit den Security Analytics her.
    - Letztes Status-Update - Der aktuelle Status.
  - Überblick über den Aktivierungsstatus des Vorfall-Sensors
- 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.



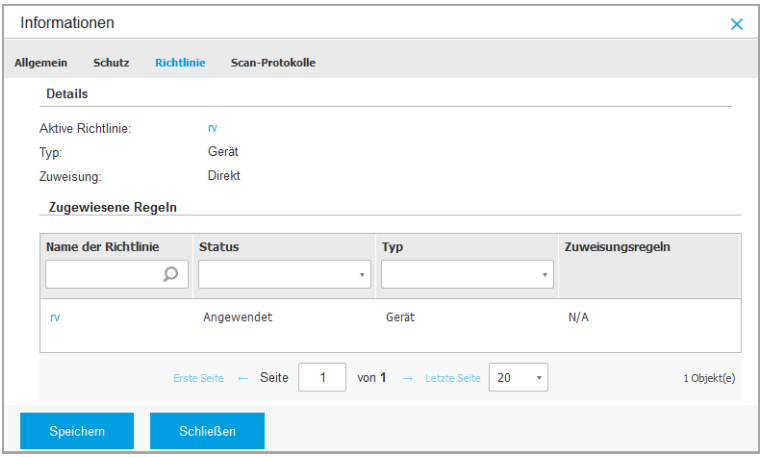
Fenster Informationen - Reiter Schutz

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.

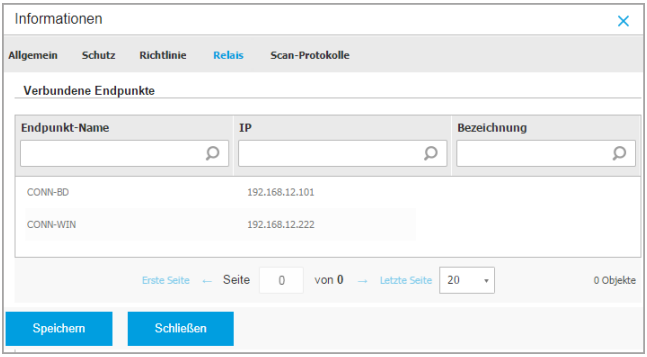


Fenster Informationen - Reiter Richtlinie

Weitere Informationen zu den Richtlinien finden Sie unter„Richtlinieneinstellungen ändern“ (S. 139)

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.

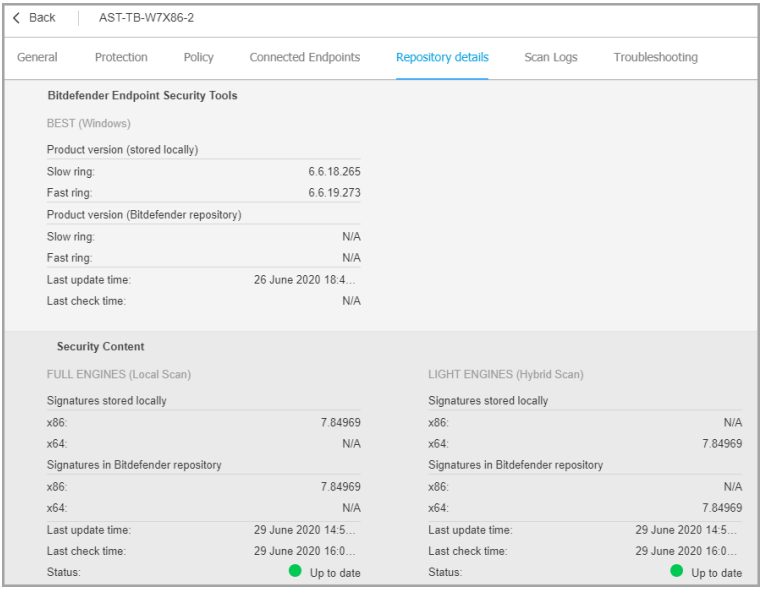


Informationsfenster - Reiter Verbundene Endpunkte

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.



Informationsfenster - Reiter Repository-Details

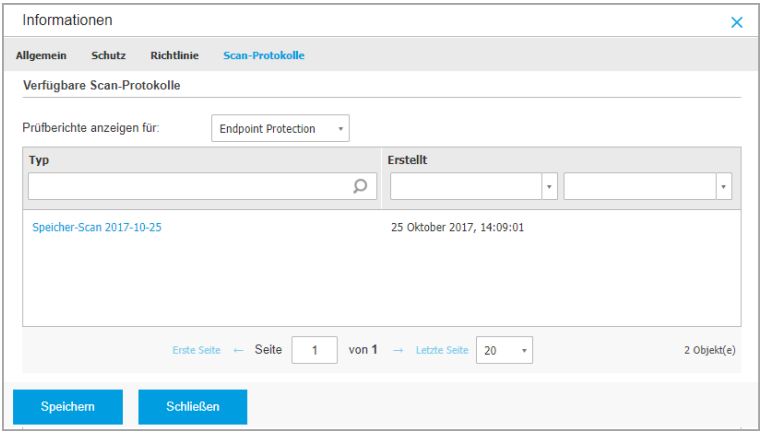
Reiter Scan-Protokolle

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 Klappmenü 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.

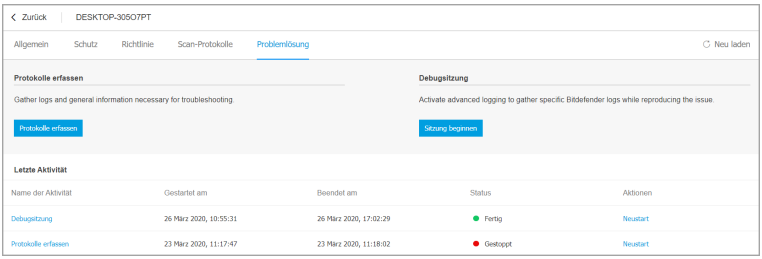


Fenster Informationen - Reiter Scan-Protokolle

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 Security Server Multi-Platform-Maschinen verfügbar.



Informationsfenster - Reiter Problemlösung

- **Protokolle erfassen**

  Mit dieser Option können Sie eine Reihe von Protokollen und allgemeinen Informationen sammeln, die für die Problembehebung 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 Problembehebung 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.
     - **Bitdefender-Cloud**: Das Protokollarchiv wird an einem Speicherort in der Bitdefender-Cloud gespeichert. Dort kann das Enterprise-Support-Team auf die Dateien zugreifen.

     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 ein (lokaler Pfad, Zugangsdaten für die Netzwerkfreigabe, Pfad zum freigegebenen Speicherort, Fallkennung).
4. Klicken Sie auf die Schaltfläche **Protokolle erfassen**.

> **Beachten Sie**
> Wenn Sie **Bitdefender-Cloud** als Speicheroption wählen, bedenken Sie bitte Folgendes:
>
> – Das Protokollarchiv wird mit identischem Namen sowohl in der **Bitdefender-Cloud** als auch auf dem Zielcomputer gespeichert. Wenn Sie auf das Problembehandlungsereignis klicken, wird ein Detailfenster mit dem Archivnahmen angezeigt.
>
> – Bitte stellen Sie dem Bitdefender-Enterprise-Support, nachdem das Archiv hochgeladen wurde, die nötigen Informationen für den geöffneten Fall zur Verfügung (Name des Zielcomputers und des Archivs). Wenn noch kein Fall besteht, öffnen Sie einfach einen neuen!

- **Debugsitzung**

  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 Problembehebung 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)	– Allgemeine Verlangsamung des Endpunkts – Die Antwort eines Programms oder einer Systemressource dauert zu lange

Problemart	Anwendungsfall
	– Ein Scanvorgang dauert länger als üblich – Keine Verbindung zum Host-Sicherheitsdienst
Update-Fehler	– Bei Aktualisierungen des Produkts oder von Sicherheitsinhalten empfangene Fehlermeldungen
Inhaltssteuerung (Datenverkehr-Scan und Benutzersteuerung)	– Website lädt nicht – Elemente der Webseite werden nicht richtig angezeigt
Konnektivität der Cloud-Dienste	– Der Endpunkt hat keine Verbindung zu den Bitdefender Cloud-Diensten
Allgemeine Produktprobleme (ausführliche Protokolle)	– Reproduktion eines generischen gemeldeten Problems mit der ausführlichen Protokollierung

Problemtypen bei Linux-Maschinen:

Problemart	Anwendungsfall
Malware-Schutz und Update	– 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)	– Reproduktion eines generischen gemeldeten Problems mit der ausführlichen Protokollierung

Problemtypen bei Security-Servern:

Problemart	Anwendungsfall
Malware-Schutz (Zugriff- und Bedarf-Scans)	Sämtliches unerwartetes Verhalten des Security-Servers, d. h.: – 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	Sämtliches in der GravityZone-Konsole beobachtetes unerwartetes Verhalten: – 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 **Beachten Sie** Setzen Sie diese Methode nur auf Empfehlung des Bitdefender-Enterprise-Supports ein.

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.
- **Bitdefender-Cloud**: Das Protokollarchiv wird an einem Speicherort in der Bitdefender-Cloud gespeichert. Dort kann das Enterprise-Support-Team auf die Dateien zugreifen.

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 ein (lokaler Pfad, Zugangsdaten für die Netzwerkfreigabe, Pfad zum freigegebenen Speicherort, Fallkennung).
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.

6.3. Endpunkte in Gruppen organisieren

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

Sie können Endpunktgruppen im linken Fenster der Seite **Netzwerk** im Ordner **Computer und Gruppen** verwalten.

Unter der **Netzwerk**gruppe, die zu Ihrem Unternehmen gehört, können Sie Computer-Gruppen innerhalb einer benutzerdefinierten Baumstruktur erstellen, löschen, umbenennen und verschieben.

Beachten Sie

- Eine Gruppe kann sowohl Endpunkte als auch andere Gruppen enthalten.
- Wenn Sie im linken Fenster eine Gruppe auswählen, können Sie alle enthaltenen Endpunkt einsehen - außer denen, die in die jeweiligen Untergruppen eingeordnet wurden. Wenn Sie alle Endpunkte 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 im rechten Fenster den Ordner **Computer und Gruppen**.
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**

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 Endpunkte verschieben

Sie können Entitäten irgendwo innerhalb der Gruppenhierarchie nach **Computer und Gruppen** verschieben. Ziehen Sie die gewünschte Entität einfach mit der Maus aus dem rechten Fenster in die gewünschten 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. 129).

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**.

6.4. Sortieren, Filtern und Suchen von Endpunkten

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 Endpunkt suchen oder nur verwaltete Endpunkte anzeigen.

6.4.1. Endpunkte sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Wenn Sie

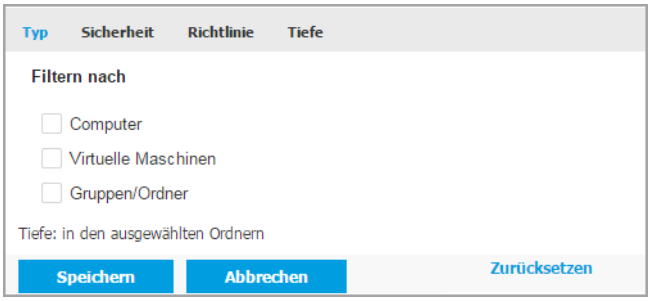
zum Beispiel möchten, dass die Endpunkte nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**. Wenn Sie erneut auf den Titel klicken, werden die Endpunkte in umgekehrter Reihenfolge angezeigt.

Computer sortieren

6.4.2. Endpunkte filtern

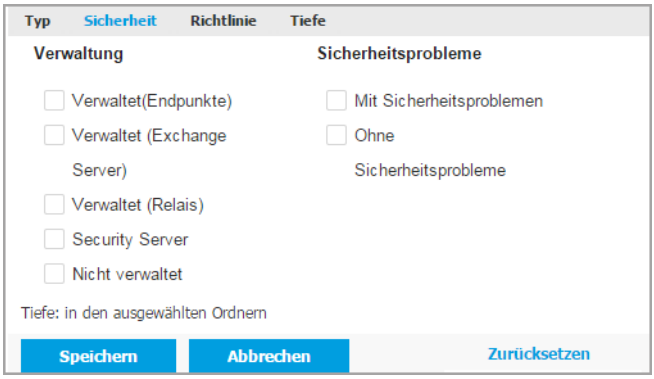
Ihre Netzwerkentitäten können Sie filtern, indem Sie im oberen Bereich der Netzwerkfenster das **Filter**-Menü verwenden.

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).



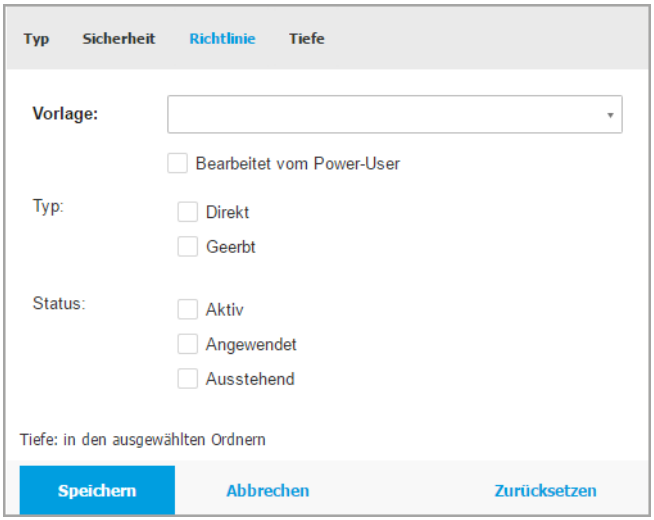
Endpunkte - Nach Typ filtern

   - **Sicherheit**. Zeigen Sie Endpunkte nach Schutzverwaltung, Sicherheitsstatus oder Ausstehende Aktivität an.



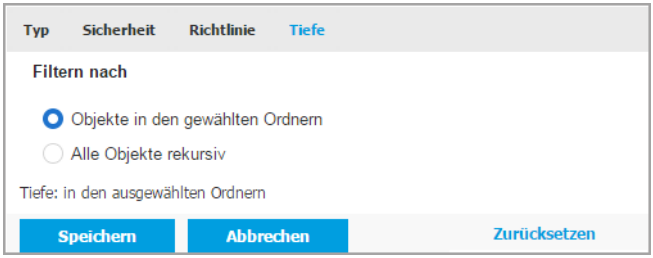
Endpunkte - nach Sicherheit filtern

- **Richtlinie**. Wählen Sie die Richtlinienvorlage, nach der Sie die Endpunkte 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.



Endpunkte - Nach Richtlinie filtern

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



Endpunkte - 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.

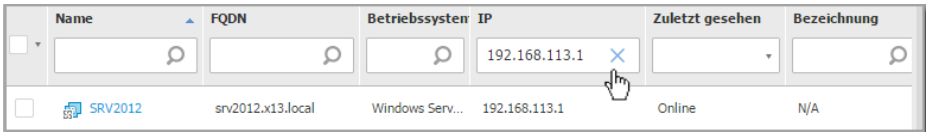
Beachten Sie
Die ausgewählten Filterkriterien werden im unteren Teil des **Filter**-Fensters angezeigt.
Klicken Sie auf **Zurücksetzen**, um alle Filter zu löschen.

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

6.4.3. Nach Endpunkten 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 Endpunktes, den Sie suchen, in das Feld **IP** ein. Nur der passende Endpunkt wird in der Tabelle angezeigt.

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



Nach Endpunkten suchen

6.5. Patch-Inventar

GravityZone findet alle von Ihrer Software benötigten Patches durch **Patch-Scan**-Aufgaben und fügt sie dann dem Patch-Inventar hinzu.

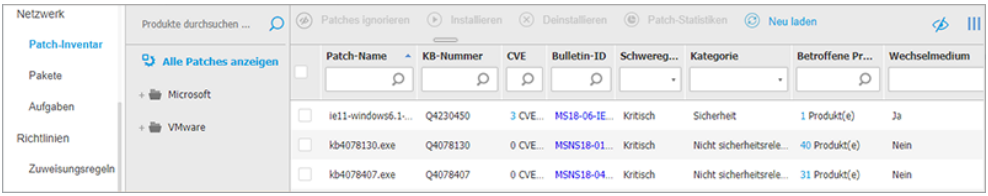
Auf der Seite **Patch-Inventar** werden alle Patches angezeigt, die für die auf Ihren Endpunkten installierte Software gefunden wurden. Für die Patches stehen Ihnen verschiedene Aktionen zur Auswahl.

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.



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

6.5.1. 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.
- **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 entfernbar 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 **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.

6.5.2. 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.

6.5.3. 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. 77)
- 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.

6.5.4. 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. 110).
- 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. 148).

4. Klicken Sie auf **Installieren**.

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

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. 95).
- 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.

6.5.5. Deinstallieren von Patches

Es kann vorkommen, dass Sie Patches, die Fehlfunktionen auf den Zielendpunkten 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 Enfernbarkeit zu filtern.

Beachten Sie
Ob ein Patch entfernbar 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, dass 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.

   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. 110).

  – 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. 148).

- 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.

6.5.6. 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.

6.6. Aufgaben ausführen

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

Sie haben die folgenden Möglichkeiten:

- „Scan“ (S. 79)
- „Nach IOCs suchen“ (S. 89)
- „Risiko-Scan“ (S. 92)
- „Patch-Aufgaben“ (S. 93)
- „Exchange-Scan“ (S. 96)
- „Installieren“ (S. 101)
- „Client Deinstallieren“ (S. 106)
- „Client aktualisieren“ (S. 106)
- „Client neu konfigurieren “ (S. 107)
- „Client reparieren“ (S. 109)
- „Computer neu starten“ (S. 110)
- „Netzwerkerkennung“ (S. 111)
- „Security Server aktualisieren“ (S. 111)

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

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

Bei einer Gruppe wird die ausgewählte Aufgabe nur für kompatible Endpunkte erstellt. Wenn kein Endpunkt 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 Endpunkten, die online sind. Wenn ein Endpunkt offline ist, wird die Aufgabe ausgeführt, sobald er wieder online ist.

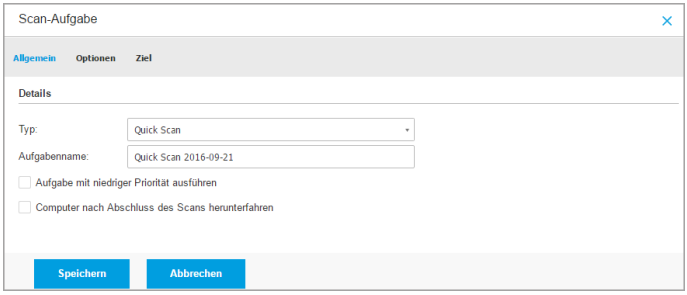
Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

Scan

So führen Sie eine Scan-Aufgabe per Fernzugriff auf einem oder mehreren Endpunkten aus:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte oder Gruppen, die Sie scannen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Scan**.

   Ein Konfigurationsfenster wird sich öffnen.
5. 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 - 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 Virenscan 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 Endpunktes 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.

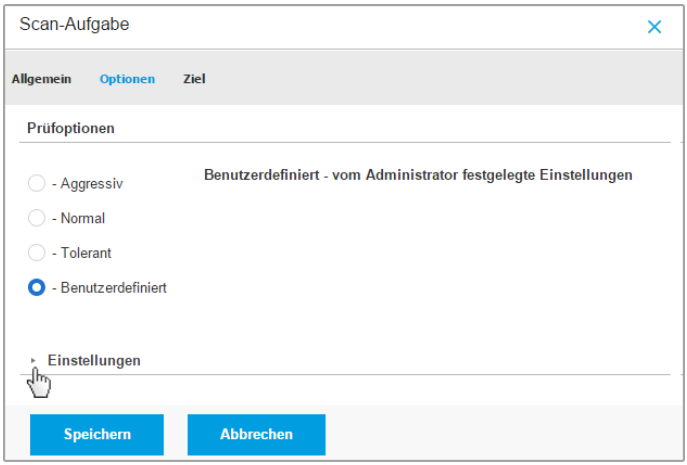
  Beachten Sie
  Diese Option gilt für Bitdefender Endpoint Security Tools und Endpoint Security (Legacy-Agent) und Endpoint Security for Mac.

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 - Konfiguration eines benutzerdefinierten Scans

Die folgenden Optionen stehen zur Verfügung:

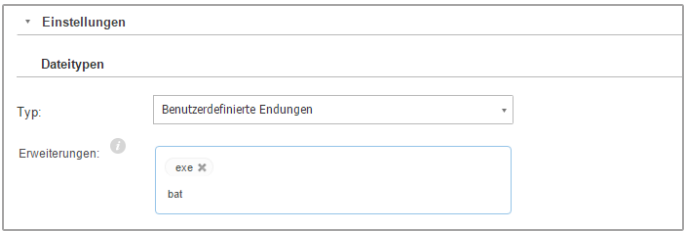
- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateiendung), oder nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für 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 im Kapitel „Anwendungsdateitypen“ (S. 483).

  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.



Optionen für eine 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 infizierten 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 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.

  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 Endpunkt 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 verdächtigte 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-Wekzeuge, 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 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 konfigurieren, die auf den Ziel-Endpunkten 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.

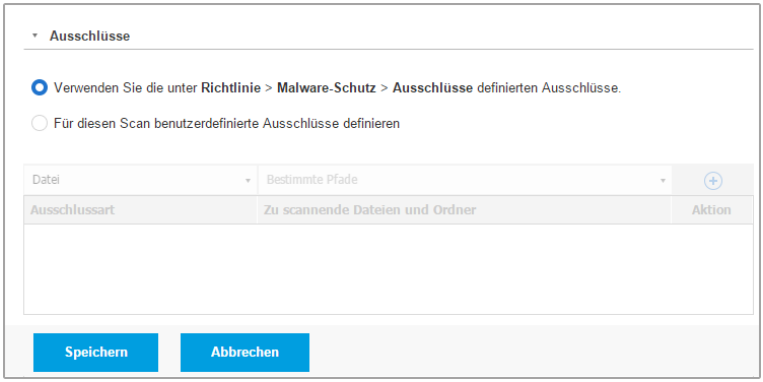
- Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist. Weitere Informationen zu den Systemvariablen finden Sie unter „Systemvariablen“ (S. 485).

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.



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. 189).

6. 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.

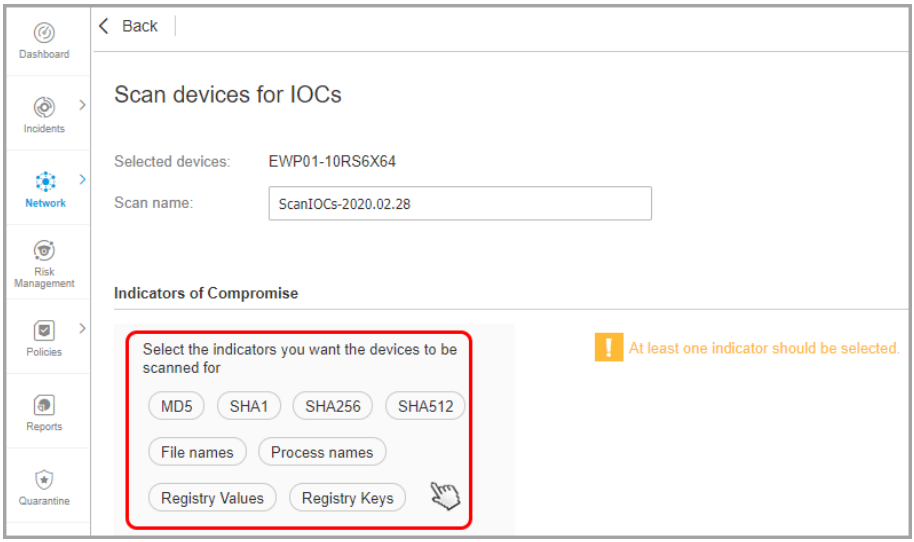
Beachten Sie
Zum Planen von Scan-Aufgaben öffnen Sie die Seite **Richtlinien**, wählen Sie die dem entsprechenden Computer zugewiesene Richtlinie aus und fügen Sie im Bereich **Malware-Schutz > Bei Bedarf** eine Scan-Aufgabe hinzu. Weitere Informationen finden Sie unter „Bedarf-Scan“ (S. 170).

6.6.2. Nach IOCs suchen

Sie können jederzeit auf den ausgewählten Endpunkten einen Bedarf-Scan auf bekannte Gefährdungsanzeichen (IOC) durchführen. Gehen Sie dazu wie folgt vor:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie aus den vorhandenen Containern die Endpunkte, die Sie scannen möchten.
3. Klicken Sie auf die Schaltfläche **Aufgaben** und wählen Sie dann den Punkt **Nach IOCs suchen**.

   Eine Konfigurationsseite wird angezeigt, auf der Sie die Art von Indikatoren auswählen müssen, die beim IOC-Scan berücksichtigt werden sollen.



Konfiguration der Suche nach IOCs

Beachten Sie
Sie müssen mindestens eine Art von IOC auswählen.

4. Wählen Sie eine oder mehrere Arten von IOCs, nach denen gesucht werden soll, und geben Sie den bekannten IOC-Namen in das neu angezeigte Feld ein.

IOCs hinzufügen

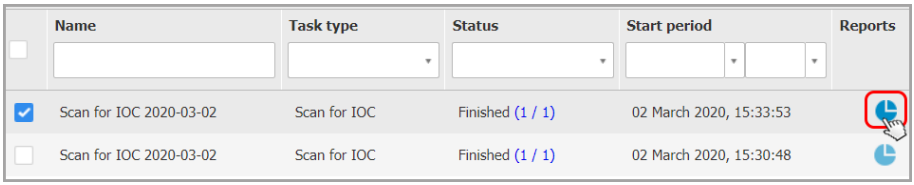
Sie können einen oder mehrere der folgenden IOC-Typen auswählen:

- MD5
- SHA1
- SHA256
- SHA512
- Dateinamen
- Prozessnamen
- Registrierungswerte
- Registry-Schlüssel

Beachten Sie
Achten Sie darauf, dass Sie nur gültige Eingaben machen. Sollte das nicht der Fall sein, wird eine entsprechende Meldung angezeigt.

5. Klicken Sie auf **Speichern**. Damit erstellen Sie die Aufgabe **Nach IOCs suchen**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk/Aufgaben** wird der Fortschritt der Aufgabe dargestellt.



Fortschrittsanzeige der Aufgaben

6. Nach Abschluss der Aufgabe können Sie auf die Schaltfläche **Berichte** klicken, um den erstellten Bericht zu lesen und die Auswirkungen des untersuchten IOC zu beurteilen.

Als Dateiendung können Sie eine oder mehrere der Folgenden wählen: `exe`, `dll`, `com`, `scr`, `jar`, `msi`, `msc`, `bat`, `ps1`, `vbs`, `vbe`, `js`, `jse`, `wsf`, `wsh`, `psc1`, `lnk`, `doc`, `docx`, `docm`, `xls`, `xlsx`, `xlsm`, `ppt`, `pptx`, `pptm`, `eml`, `rtf`, `pdf`, `html`, `ppsx`, `pps`, `ppsm`, `pot`, `potx`, `potm`, `ocx`, `sys`, `fnr`, `fne` und `pif`.

Mit der Aufgabe **Nach IOCs suchen** werden die folgenden Speicherorte durchsucht:

- %Windows%\System32\Drivers
- %Windows%\System32\WindowsPowerShell\v1.0
- %Windows%\system32\config\systemprofile\AppData
- %Windows%\System32\Tasks
- %Windows%\System32\wbem
- %Windows%\SysWOW64\WindowsPowerShell\v1.0
- %Windows%\SysWOW64\config\systemprofile\AppData
- %Windows%\SysWOW64\sysprep
- %Windows%\Scripts
- %Windows%\System
- %Windows%\Web
- %Users%

Wichtig
Die **Nach IOC suchen**-Aufgaben werden in den folgenden Situationen auf den Endpunkten nicht ausgeführt bzw. schlagen fehl:

- Auf dem Endpunkt läuft kein Windows-Betriebssystem.
- Die Bitdefender-Agentenlizenz des Endpunkts ist ungültig.
- Im BEST-Client, der auf den Endpunkten installiert ist, ist das **EDR**-Modul nicht installiert.
- Es befinden sich mehr als 100 **Nach IOCs suchen**-Aufgaben in der Warteschlange.
- Auf der Konfigurationsseite der **Nach IOCs suchen**-Aufgabe wurden ungültige Eingaben gemacht.

6.6.3. Risiko-Scan

Sie können jederzeit bei Bedarf auf ausgewählten Endpunkten Risiko-Scan-Aufgaben ausführen. Gehen Sie dazu wie folgt vor:

1. Gehen Sie zur Seite **Netzwerk**.
2. Durchsuchen Sie die Container im linken Bereich und wählen Sie die Endpunkte aus, die Sie scannen möchten.

3. Klicken Sie auf die Schaltfläche **Aufgaben** und wählen Sie dann den Punkt **Risiko-Scan**.

   Es wird eine Meldung angezeigt, in der Sie die Ausführung der Risiko-Scan-Aufgabe bestätigen müssen.

   Beachten Sie
   Die Risiko-Scan-Aufgabe wird für alle standardmäßig aktivierten Risikoindikatoren ausgeführt.

4. Nachdem die Aufgabe erfolgreich abgeschlossen wurde, können Sie diese Indikatoren im Reiter Fehlkonfigurationen auf der Seite **Sicherheitsrisiken** analysieren und ggf. auswählen, welche Indikatoren ignoriert werden sollen.

   Der allgemeine Risikobewertung des Unternehmens wird auf Grundlage der ignorierten Risikoindikatoren erneut berechnet.

   Beachten Sie
   Die vollständige Liste der Indikatoren und deren Beschreibung finden Sie in diesem Artikel in der Wissensdatenbank.

Wichtig
Die **Risiko-Scan**-Aufgaben werden in den folgenden Situationen auf den Endpunkten nicht ausgeführt / schlagen fehl:

- Auf dem Endpunkt läuft kein Windows-Betriebssystem.
- Die Bitdefender-Agentenlizenz des Endpunkts ist ungültig.
- Für die auf den Endpunkt angewandten Richtlinie ist das Modul Risiko-Management deaktiviert.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

6.6.4. 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. 69).

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. 235).

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 alles 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 ausführen“ (S. 78).

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. 235).
- 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. 73).
- 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.

6.6.5. 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 im Kapitel „Scannen des Exchange-Informationsspeichers“ (S. 255).

So scannen Sie eine Exchange-Server-Datenbank:

1. Gehen Sie zur Seite **Netzwerk**.
2. 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.

3. Markieren Sie das Kästchen des Exchange-Servers, dessen Datenbank Sie scannen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Exchange-Scan**. Ein Konfigurationsfenster wird sich öffnen.
5. 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 im Kapitel „Anwendungsdateitypen“ (S. 483).

    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 verdächtigte 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**.

6. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.
7. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

6.6.6. Installieren

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

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

Die Bitdefender-Sicherheitssoftware kann per Fernzugriff über das Control Center auf Endpunkten 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-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.

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 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**.

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

   Der Assistent **Client installieren** wird angezeigt.

Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

6. 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.

7. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.
8. 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.

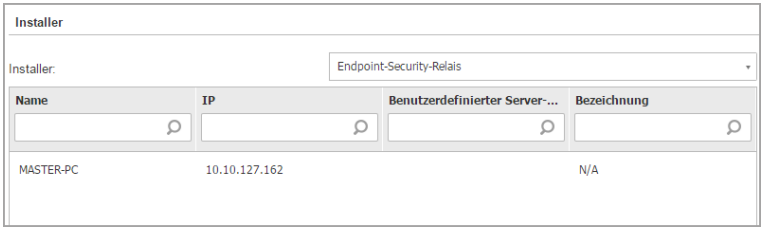
> **Wichtig**
> Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

9. 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.

10. Konfigurieren Sie im Bereich **Installer** das Relais, zu dem die Endpunkte eine Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren:

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



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 bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.
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.

    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.

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.

6.6.7. 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. 428).

6.6.8. Client Deinstallieren

So entfernen Sie die Bitdefender-Sicherheitssoftware per Fernzugriff:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client deinstallieren**.
5. Ein Konfigurationsfenster wird angezeigt, in dem Sie sich für den Verbleib Quarantäne-Objekte auf der Client-Maschine entscheiden können.
6. 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.

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

6.6.9. 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 im Kapitel „Sicherheitsstatus“ (S. 47).

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 den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, auf denen Sie ein Client-Update durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Update**. Ein Konfigurationsfenster wird sich öffnen.
5. Sie können nur das Produkt, nur die Sicherheitsinhalte oder beides aktualisieren.
6. 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.

6.6.10. 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 Endpunkte:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, bei denen Sie die Installationseinstellungen ändern möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Client neu konfigurieren**.
5. 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.
6. 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.

7. 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.
8. 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.

9. 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).
10. 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.

6.6.11. Client reparieren

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

Beachten Sie
- The modules currently configured on the agent will not be changed.
- Die Reparaturaufgabe setzt den Sicherheitsagenten auf die aktuelle Slow-Ring-Version zurück.

So übermitteln Sie die Aufgabe Client reparieren an einen Client:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, auf denen Sie die Client-Reparatur durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Client reparieren**. Ein Bestätigungsfenster wird angezeigt.

5. Markieren Sie das Kästchen **Ich habe das verstanden und stimme dem zu** und klicken Sie auf die Schaltfläche **Speichern**, um die Aufgabe auszuführen.

   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.

6.6.12. Computer neu starten

Sie können verwaltete Endpunkte aus der Ferne neu starten.

Beachten Sie
Bevor Sie einzelne Endpunkte neu starten, sollten Sie einen Blick auf die Seite **Netzwerk > Aufgaben** werfen. Zuvor erstellte Aufgaben könnten derzeit noch auf den ausgewählten Endpunkten laufen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, die Sie neu starten möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Computer neu starten**.
5. Wählen Sie den Zeitpunkt des Neustarts:
   - Wählen Sie **Jetzt neu starten**, um die Endpunkte sofort neu zu starten.
   - Wählen Sie **Neustart am**, und nutzen Sie die Eingabefelder weiter unten, um den Neustart für einen bestimmten Zeitpunkt zu planen.
6. 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.

6.6.13. Netzwerkerkennung

Die Netzwerkerkennung wird automatisch stündlich von Sicherheitsagenten mit Relais-Rolle durchgeführt. Sie können aber auch jederzeit manuell eine Netzwerkerkennungsaufgabe über das Control Center einer beliebigen durch Bitdefender Endpoint Security Tools geschützten Maschine durchführen.

So führen Sie eine Netzwerkerkennungsaufgabe in Ihrem Netzwerk durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen des Relais-Endpunktes, über den Sie eine Netzwerkerkennung durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Netzwerkerkennung**.
5. 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.

6.6.14. Security Server aktualisieren

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

1. Gehen Sie zur Seite **Netzwerk**.
2. 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**.
3. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der Tabelle, und wählen Sie **Security Server aktualisieren**.
4. 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.

6.7.1. Integration mit Active Directory

Über die Integration kann GravityZone das Computerinventar von Active Directory (sowohl unternehmensintern installiert als auch aus Microsoft Azure) importieren. So können Sie ganz unkompliziert den Bitdefender-Schutz auf Active-Directory-Endpunkten installieren und verwalten. Die Integration erfolgt über einen verwalteten Endpunkt namens Active-Directory-Integrator.

So können Sie die Active-Directory-Integration verwalten:

- Einrichtung des Active-Directory-Integrators
- Entfernen des Active-Directory-Integrators
- Integration entfernen

Einrichtung des Active-Directory-Integrators

Sie können für jede verfügbare Domain einen oder mehrere Active-Directory-Integratoren definieren.

Vorbereitende Maßnahmen

Der Active-Directory-Integrator muss die folgenden Anforderungen erfüllen:

- Auf ihm muss Windows laufen.
- Er ist im Active Directory verknüpft.
- Er wird von Bitdefender Endpoint Security Tools geschützt.
- Er ist immer online. Wenn nicht, kann die Synchronisation mit Active Directory beeinträchtigt werden.

Wichtig
Es wird empfohlen, dass Endpunkten, die im Active Directory verknüpft sind, die Richtlinie direkt zugewiesen wird. Alle in der Active-Directory-Domäne gefundenen Endpunkte werden von ihrem Ursprungsordner in den Active-Directory-Ordner verschoben. In diesem Fall und wenn diese Endpunkte über eine geerbte Richtlinie verfügen, wird ihnen diese Richtlinie standardmäßig zugewiesen.

Einrichtung des Active-Directory-Integrators

Sie können für jede verfügbare Domain einen oder mehrere Active-Directory-Integratoren definieren.

So richten Sie einen Endpunkt als Active-Directory-Integrator ein:

1. Gehen Sie zur Seite **Netzwerk**.
2. Finden Sie im Netzwerkinventar die Gruppe, in der sich der Endpunkt befindet, und markieren Sie ihn.

   Beachten Sie
   Wenn Sie mehr als einen Integrator definieren möchten, müssen Sie dazu einen Endpunkt nach dem anderen auswählen.

3. Klicken Sie auf die Schaltfläche **Integrationen** am oberen Rand der Tabelle, und wählen Sie **Als Active-Directory-Integrator einrichten**.
4. Bestätigen Sie die Aktion, indem Sie auf **Ja** klicken.

   An dem neuen Symbol erkennen Sie, dass dieser Endpunkt jetzt ein Active-Directory-Integrator ist. Nach einigen Minuten wird der **Active Directory**-Baum neben **Computer und Gruppen** angezeigt. Bei großen Active-Directory-Netzwerken kann die Synchronisation eine Weile dauern. Endpunkte in derselben Domain wie der Active-Directory-Integrator werden von **Computer und Gruppen** in den Active-Directory-Container verschoben.

Synchronisation mit Active Directory

GravityZone wird automatisch jede Stunde mit Active Directory synchronisiert.

GravityZone kann in den folgenden Fällen die Synchronisation mit Active Directory nicht durchführen:

- Alle Active-Directory-Integrator-Rollen wurden entfernt
- Die Verbindung zwischen Active-Directory-Integratoren und GravityZone wurde für mindestens 2 Stunden unterbrochen.
- Keiner der Active-Directory-Integratoren derselben Domain kann mit dem Domain Controller kommunizieren.

In jedem dieser Fälle wird im **Infobereich** ein Active-Directory-Problem gemeldet. Weitere Informationen finden Sie unter „Benachrichtigungen“ (S. 460).

Entfernen des Active-Directory-Integrators

So entfernen Sie die Active-Directory-Integrator-Rolle von einem Endpunkt:

1. Gehen Sie zur Seite **Netzwerk**.
2. Finden Sie im Netzwerkinventar die Gruppe, in der sich der Active-Directory-Integrator befindet, und markieren Sie ihn.

   Beachten Sie
   Wenn Sie mehrere Integratoren entfernen möchten, müssen Sie einen Endpunkt nach dem anderen auswählen.

3. Klicken Sie auf die Schaltfläche **Integrationen** am oberen Rand der Tabelle, und wählen Sie **Active-Directory-Integrator entfernen**.
4. Eine Bestätigungsmeldung wird angezeigt.
   - Falls sich ein weiterer Endpunkt mit der Active-Directory-Integrator-Rolle in derselben Domain befindet, enthält die Bestätigungsmeldung einen Warnhinweis, dass die aktuelle Domain nicht mehr mit GravityZone synchronisiert wird.
   - Wenn der Endpunkt offline ist, wird die Active-Directory-Integrator-Rolle entfernt, sobald er wieder eingeschaltet wird.

Im Bereich **Benutzeraktivität** können Sie überprüfen, ob ein Active-Directory-Integrator von Ihrem verwalteten Netzwerk entfernt wurde, indem Sie die Benutzerprotokolle anhand der folgenden Kriterien filtern:

- **Bereich**: Active Directory
- **Aktion**: Active-Directory-Integrator entfernt

Weitere Informationen finden Sie im Kapitel „Benutzeraktivitätsprotokoll“ (S. 457).

Entfernen der Active-Directory-Integration

So entfernen Sie eine oder mehrere Domains aus dem Active-Directory-Ordner:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie unter dem **Netzwerk**-Baum im linken Fenster den Ordner **Active Directory** aus.
3. Wählen Sie im rechten Fenster den Order der Domain, die Sie entfernen möchten.

4. Klicken Sie auf die Schaltfläche **Integrationen** am oberen Rand der Tabelle, und wählen Sie **Active-Directory-Integration entfernen**.
5. Eine Bestätigungsmeldung wird angezeigt. Eine Option in dieser Meldung lässt Sie wählen, ob Sie die nicht verwalteten Endpunkte aus dem Netzwerkinventar entfernen möchten oder nicht. Vorsicht: Diese Option ist standardmäßig aktiviert. Klicken Sie auf **Bestätigen**, um fortzufahren.
6. Alle Endpunkte unter der ausgewählten Domain werden im Ordner **Computer und Gruppen** (oder in ihren ursprünglichen Gruppen) abgelegt, und die Active-Directory-Integrator-Rolle wird von den entsprechenden Endpunkten dieser Domain entfernt.

6.8. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte zu verwalteten Endpunkten erstellen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

   Wenn Sie möchten, können Sie den Inhalt der ausgewählten Gruppe nur nach verwalteten Endpunkten filtern.
3. Markieren Sie die Kästchen der Computer, die im Bericht enthalten sein sollen.
4. Klicken Sie auf die Schaltfläche **Bericht** am oberen Rand der Tabelle, und wählen Sie den Berichtstyp aus dem Menü.

   Weitere Informationen finden Sie im Kapitel „Berichte zu Computern und virtuellen Maschinen“ (S. 411).
5. Konfigurieren Sie die Berichtsoptionen. Weitere Informationen finden Sie im Kapitel „Berichte erstellen“ (S. 428).
6. Klicken Sie auf **Generieren**. Der Bericht wird sofort angezeigt.

   Es dauert unterschiedlich lange, bis Berichte erstellt sind, je nach Anzahl der gewählten Endpunkte.

6.9. Richtlinien zuweisen

Über Richtlinien können Sie Sicherheitseinstellungen auf Endpunkten verwalten.

Auf der Seite **Netzwerk** können Sie Richtlinien für jeden Endpunkt bzw. jede Gruppe von Endpunkten anzeigen, ändern und zuweisen.

Beachten Sie
Sicherheitseinstellungen stehen nur für verwaltete Endpunkte zur Verfügung. Um Sicherheitseinstellungen leichter überblicken und verwalten zu können, können Sie das Netzwerkinventar auch nach verwalteten Endpunkten Filtern.

So zeigen Sie die Richtlinie an, die einem bestimmten Endpunkt zugewiesen wurde:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Klicken Sie auf den Namen des verwalteten Endpunktes, der Sie interessiert. Es öffnet sich ein Informationsfenster.
4. Klicken Sie im Reiter **Allgemein** des Bereichs **Richtlinie** auf den Namen der aktuellen Richtlinie, um ihre Einstellungen anzuzeigen.
5. 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 Endpunkte auswirken, denen diese Richtlinie zugewiesen wurde.

   Weitere Informationen zur Änderung von Richtlinieneinstellungen finden Sie unter „Richtlinien für Computer und virtuelle Maschinen“ (S. 141).

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

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie das Kästchen des gewünschten Endpunkts bzw. der gewünschten Gruppe. Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
4. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** am oberen Ende der Tabelle.
5. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor. Weitere Informationen finden Sie im Kapitel „Richtlinien zuweisen“ (S. 131).

6.10.1. 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. 279).

6.11. 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 im linken Fenster die gewünschte Netzwerkgruppe.

   Beachten Sie
   Sie können unter **Computer und Gruppen** nur solche Endpunkte löschen, die außerhalb von integrierten Netzwerkinfrastrukturen gefunden wurden.

3. Markieren Sie im rechten Fenster das Kästchen des Endpunktes, den 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**.

   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.
5. Der Endpunkt wird in den Ordner **Gelöscht** verschoben.

Sie können Endpunkte aus dem Ordner **Gelöscht** jederzeit mit der Maus in **Computer und 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.

6.12. 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.

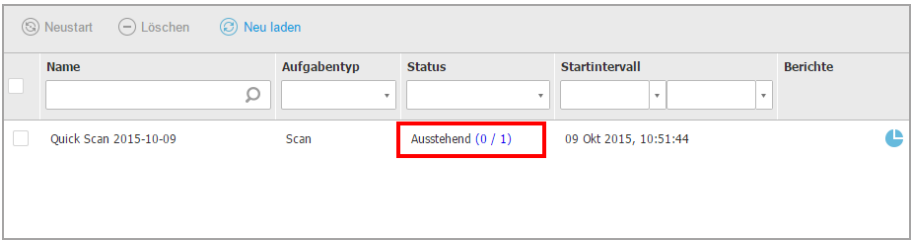
Auf der Seite **Netzwerk > Aufgaben** haben Sie folgende Möglichkeiten:

- Aufgabenstatus überprüfen
- Aufgabenberichte anzeigen
- Aufgaben neu starten
- Exchange-Scan-Aufgaben anhalten
- Aufgaben löschen

6.12.1. 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.



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 bisher keine der Teilaufgaben gestartet wurde.
  - **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 Exchance-Bedarf-Scan-Aufgaben können Sie zusätzlich den Abschlussstatus anzeigen.

  - **Fertig** - wenn die Teilaufgabe erfolgreich abgeschlossen wurde.

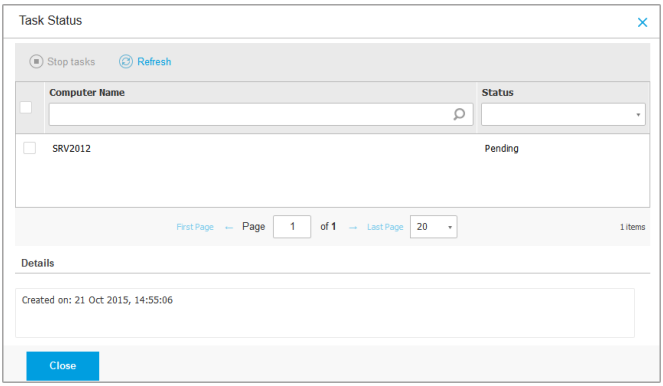
  - **Ausstehend** - wenn die Teilaufgabe noch nicht gestartet wurde. Das kann in den folgenden Situationen passieren:

- Die Teilaufgabe wartet in einer Warteschlange.
- Es gibt Verbindungsprobleme zwischen der Control Center und dem Zielobjekt im Netzwerk.

– **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.



Aufgabenstatusdetails

Dort finden Sie die folgenden Informationen:

– Datum und Uhrzeit des Aufgabenstarts.

– Datum und Uhrzeit des Aufgabenendes.

– Beschreibung aufgetretener Fehler.

6.12.2. Aufgabenberichte anzeigen

Auf der Seite **Netzwerk > Aufgaben** können Sie Schnellberichte zu Scan-Aufgaben lesen.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.

2. Markieren Sie das Kästchen der Scan-Aufgabe, die Sie interessiert.
3. Klicken Sie auf die entsprechende Schaltfläche in der Spalte **Berichte**. Warten Sie, bis der Bericht angezeigt wird. Weitere Informationen finden Sie im Kapitel „Berichte verwenden“ (S. 410).

6.12.3. 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 wir folgt neu starten:

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie die Kästchen für die fehlgeschlagenen Aufgaben.
3. 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.

6.12.4. 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. Klicken Sie auf den Link in der **Status**-Spalte, um das **Augabenstatus**-Fenster zu öffnen.
3. Aktivieren Sie die Kästchen für die ausstehende oder laufende Unteraufgabe, die Sie anhalten möchten.
4. 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.

6.12.5. 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. Markieren Sie das Kästchen der Aufgabe, die Sie löschen möchten.
3. 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.

6.13. 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-Bereingung

6.13.1. Netzwerkinventareinstellungen

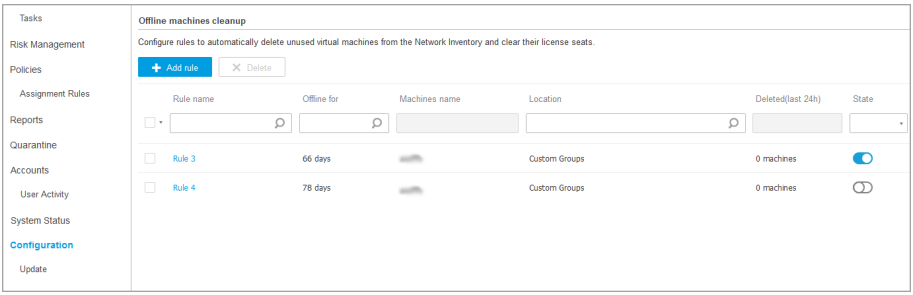
Im Abschnitt **Netzwerkinventareinstellungen** finden Sie die folgenden Optionen:

- **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**.

6.13.2. Offline-Maschinen-Bereingung

Im Abschnitt **Offline-Maschinen-Bereinigung** können Sie Regeln für das automatische Löschen ungenutzter virtueller Maschinen aus dem Netzwerkinventar anlegen.



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**.

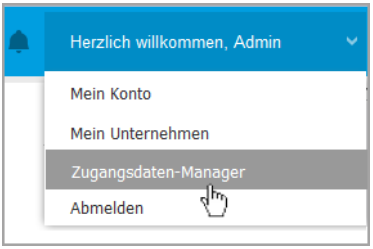
So können Sie eine oder mehrere Regeln löschen:

1. Verwenden Sie die Kästchen, um eine oder mehrere Regeln auszuwählen.
2. Klicken Sie am oberen Rand der Tabelle auf **Löschen**.

6.14. Zugangsdaten-Manager

Im Zugangsdaten-Manager können Sie die Zugangsdaten, die Sie für die Fernauthentifizierung unter den verschiedenen Betriebssystemen in Ihrem Netzwerk benötigen, definieren.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.

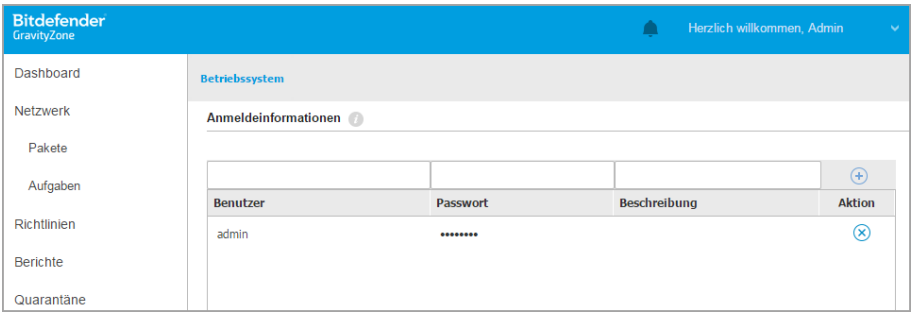


Das Zugangsdaten-Manager-Menü

6.14.1. Zugangsdaten zum Zugangsdaten-Manager hinzufügen

Mit dem Zugangsdaten-Manager 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.

6.14.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete 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

Direkt nach der Installation wird den Netzwerkinventarobjekten die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist. Die Standardrichtlinie können sie weder ändern noch löschen. Sie können Sie nur als Vorlage zur Erstellung neuer Richtlinien verwenden.

Was Sie über Richtlinien wissen sollten:

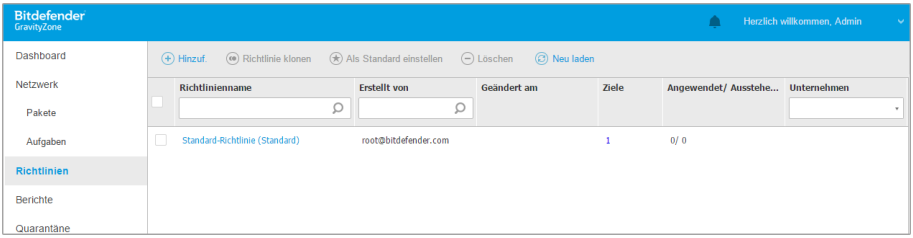
- Richtlinien werden in der **Richtlinien**übersicht erstellt und in der **Netzwerk**übersicht den Netzwerkobjekten zugewiesen.
- Richtlinien können mehrere Moduleinstellungen von anderen Richtlinien erben.
- Richtlinienzuweisung für Endpunkte können so konfiguriert werden, dass eine Richtlinie je nach Standort des Endpunkts immer gilt oder nur unter bestimmten Voraussetzungen. 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 Ihren 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.



Die Richtlinienübersicht

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.

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

1. Klicken Sie auf die Schaltfläche **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.

Sie können die bestehenden Richtlinien sortieren und über auswählbare Kriterien nach bestimmen 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 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.
3. Konfigurieren Sie die Richtlinieneinstellungen. Detaillierte Informationen finden Sie im Kapitel „Richtlinien für Computer und virtuelle Maschinen“ (S. 141).
4. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen und zur Liste der Richtlinien zurückzukehren.

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.

Es gibt zwei Möglichkeiten zur Zuordnung von Richtlinien:

- Gerätebasierte Zuweisung ermöglicht die manuelle Auswahl der gewünschten Endpunkte zur Zuweisung von Richtlinien. Diese Richtlinien werden auch Geräterichtlinien 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.

Geräterichtlinien zuweisen

In GravityZone lassen sich Richtlinien auf verschiedene Weisen zuweisen:

- Direkte Zuweisung der Richtlinie zum Ziel.

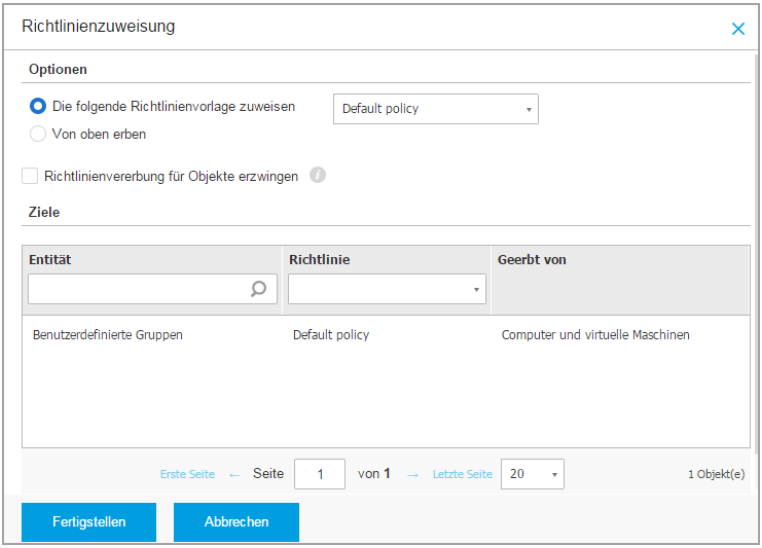
- Zuweisung der Richtlinie zur übergeordneten Gruppe mittels Vererbung.
- Richtlinienvererbung auf das Ziel erzwingen.

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 Zielendpunkte aus. Sie können einen oder mehrere Endpunkte oder Gruppen von Endpunkten auswählen.
3. 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:



Einstellungen für die Richtlinienzuweisung

4. Überprüfen Sie die Tabelle mit den Zielendpunkten. 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.

5. Wird eine Warnung angezeigt, klicken Sie zum Fortfahren auf den Link **Diese Ziele ausschließen**.
6. Wählen Sie eine der verfügbaren Optionen zur Zuordnung der Richtlinie aus:
   - **Die folgende Richtlinienvorlage zuweisen** - um den Zielendpunkten eine bestimmte Richtlinie direkt zuzuweisen.
   - **Von oben erben** - um die Richtlinie der übergeordneten Gruppe zu verwenden.
7. 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, das 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.
8. 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 Zielendpunkte 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:

Regelbasierte Richtlinien zuweisen

Auf der Seite **Richtlinien > Zuweisungsregeln** können Sie Regeln für die Richtlinienzuweisung für bestimmte Standorte definieren. Sie können zum Beispiel strengere Firewall-Regeln anwenden, falls sich der Nutzer von außerhalb des Unternehmens ins Internet einloggt; es können aber auch unterschiedliche Frequenzen für On-Demand-Aufgaben außerhalb des Unternehmens definiert werden.

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
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`
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.

Typ	Wert

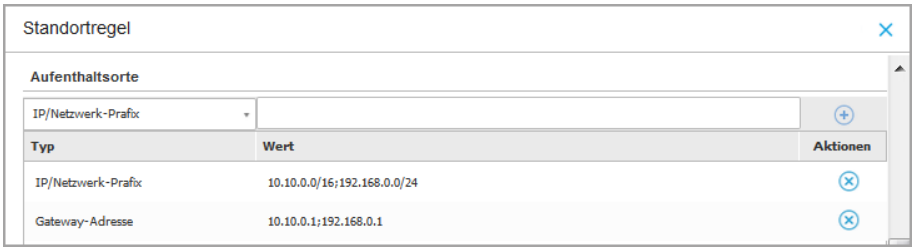
Hostname	Hostname
	Zum Beispiel: `cmp.bitdefender.com`
	
	Wichtig
	Sie können auch Platzhalter verwenden. Das Sternchen (*) ersetzt null oder mehr Zeichen und das Fragezeichen (?) ersetzt genau ein Zeichen. Beispiele:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

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

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. 135).

   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.

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. Finden Sie die Richtlinie in der Liste, und klicken Sie auf ihren Namen, um sie zu bearbeiten.
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Detaillierte Informationen finden Sie im Kapitel „Richtlinien für Computer und virtuelle Maschinen“ (S. 141).
4. 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. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinienseite.
3. Geben Sie einen neuen Namen für die Richtlinie ein.
4. Klicken Sie auf **Speichern**.

Beachten Sie
Jeder Richtlinienname 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 Richtlinie zu löschen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Markieren Sie das Kästchen der Richtlinie, die Sie löschen möchten.
3. 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. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinieneinstellungsseite
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Die Einstellungen sind in die folgenden Bereiche eingeteilt:
   - Allgemein
   - Malware-Schutz
   - Sandbox Analyzer
   - Firewall
   - Netzwerkschutz
   - Patch-Verwaltung

- Gerätesteuerung
- Relais
- Exchange-Schutz
- Verschlüsseln
- Speicherschutz
- Vorfallsensor
- Risiko-Management

Durchsuchen Sie die Bereich über das Menü links auf der Seite.

4. 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. 130).

7.2.1. Allgemein

Mithilfe der allgemeinen Einstellungen können Sie für die entsprechenden Endpunkte Anzeigeoptionen, Proxy-Einstellungen, Power-User-Einstellungen, Kommunikationsoptionen und Update-Einstellungen konfigurieren.

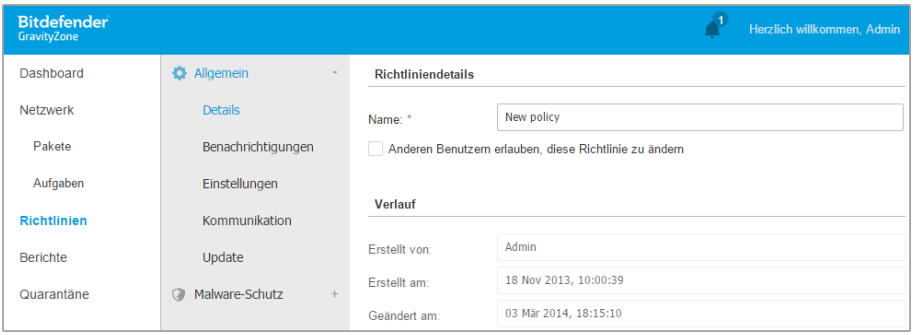
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Details
- Benachrichtigungen
- Einstellungen
- Kommunikationsserver
- Update (Aktualisierung)
- Sicherheitstelemetrie

Details

Auf der Seite **Details** finden Sie allgemeine Informationen zu den Richtlinien:

- Richtlinienname
- 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



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.

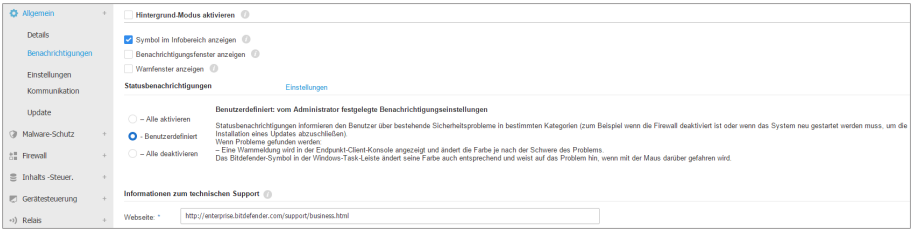
Damit die Standard-E-Mail-Anwendung auf dem Endpunkt geöffnet wird, wenn man im Bereich **Über** auf die E-Mail-Adresse klickt, müssen Sie sie im Feld **E-Mail** mit dem Präfix "mailto:" hinzufügen. Beispiel: `mailto: name@domain.com`.

Benutzer können auf diese Informationen aus der Konsole des Sicherheitsagenten zugreifen, indem sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste klicken und anschließend **Über** wählen.

Benachrichtigungen

In diesem Bereich können Sie die Anzeigeoptionen 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 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.

So wird der Benutzer nach Auswahl der Sandbox Analyzer-Kästchen zum Beispiel von Bitdefender Endpoint Security Tools informiert, wenn eine Datei zur Verhaltensanalyse übermittelt wird.

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 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.
- **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 Bitdefender-Symbol in ihrer Task-Leiste klicken und dann aus dem Kontextmenü **Power-User** de 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.

Kommunikationsserver

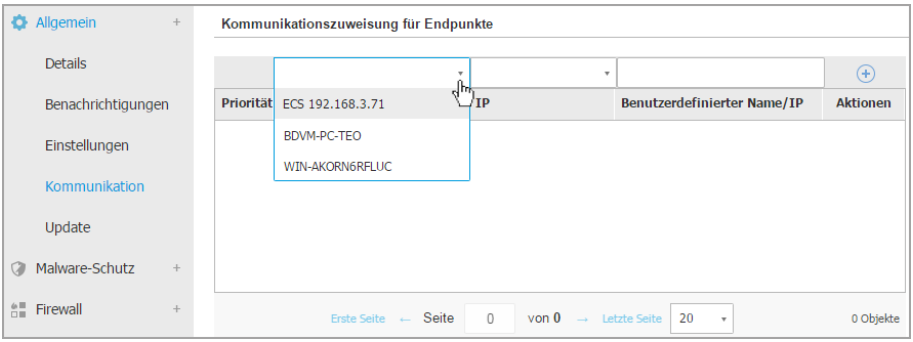
In diesem Bereich können Sie den gewünschten Endpunkten eine oder mehrere Relais-Maschinen zuweisen und dann die Proxy-Einstellungen für die Kommunikation zwischen diesen Endpunkten und der GravityZone konfigurieren.

Kommunikationszuweisung für Endpunkte

Wenn im Zielnetzwerk mehrere Relais-Agenten verfügbar sind, können Sie den ausgewählten Computern per Richtlinie einen oder mehrere Relais-Endpunkte zuweisen.

So weisen Sie Ziel-Computern Relais-Endpunkte zu:

1. Klicken Sie in der Tabelle **Kommunikationszuweisung für Endpunkte** auf das Feld **Name**. Die Liste der in Ihrem Netzwerk erkannten Relais-Endpunkte wird angezeigt.
2. Wählen Sie eine Entität.



Richtlinien - Kommunikationseinstellungen

3. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle.

   Der Relais-Endpunkt wird der Liste hinzugefügt. Alle Zielcomputer werden über die angegebenen Relais-Endpunkt mit dem Control Center kommunizieren.

4. Wiederholen Sie diese Schritte, wenn Sie mehrere Relais (sofern vorhanden) hinzufügen möchten.

5. Sie können die Priorität der Relais-Endpunkte konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile ⌃ hoch und ⌄ rnter 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.

6. 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 dem GravityZone Control Center 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:

- **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 geparst 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 - 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).

– Um mehr Kontrolle über Konfigurationsänderungen und die Aktualisierung des Bereitstellungsprozesses zu erhalten, können Sie den BEST-Agenten auf Ihren Linux-Maschinen so konfigurieren, dass er Updates des EDR-Kernel-Moduls per **Produkt-Update** ausführt.

  Wenn das Kästchen **Produkt-Update** aktiviert ist:

  - Wenn Sie das Kästchen **Linux EDR-Module mit dem Produkt-Update aktualisieren** aktivieren, aktualisiert GravityZone die Kernelversionen via **Produkt-Update**.
  - Wenn Sie diese Option nicht aktivieren, werden die Kernelversionen via **Update der Sicherheitsinhalte** aktualisiert.

  Beachten Sie
  Wenn Sie die Option **Linux EDR-Module mit dem Produkt-Update aktualisieren** aktivieren, aber die Option **Produkt-Update** deaktivieren, werden die Linux EDR-Module nicht aktualisiert.

- **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 für Bitdefender-Sicherheitsagenten ist http://upgrade.bitdefender.com. 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.

- **update.cloud.2d585.cdn.bitdefender.net**. Das ist die Bitdefender-Standard-Update-Adresse, von der aus Bitdefender Updates zur Verfügung stellt. Diese Update-Adresse sollte immer die als letzte Option in der Liste aufgeführt sein.

– Geben Sie die IP-Adresse oder den Host-Namen eines oder mehrerer Udate-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 Udpate-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.

Sicherheitstelemetrie

Beachten Sie
Diese Funktion erfordert eine EDR-Lizenz und ist nur für Windows-Endpunkte verfügbar.

Mit der Sicherheitstelemetrie haben Sie Zugriff auf zugrunde liegenden Daten zu Sicherheitsereignissen, so dass Sie benutzerdefinierte Korrelationen erstellen können.

Um optimale Leistung und geringe Datenmengen zu gewährleisten, übermitteln die Agenten nur Ereignisse, die für die Sicherheit Ihres Netzwerks relevant sind. Diese Ereignisse betreffen:

- Prozesse: erstellen, beenden
- Dateien: erstellen, lesen, ändern, verschieben, löschen
- Registrierung: Schlüssel erstellen und löschen, Wert ändern und löschen
- Benutzerzugriff: anmelden
- Netzwerkverbindung

Der Bitdefender-Agent übermittelt diese Informationen in einem branchenüblichen Standardformat (JSON, CEF) direkt an die von Ihnen verwendete SIEM-Lösung.

Konfigurieren Sie die Richtlinie wie folgt, um Sicherheitsereignisse von den Zielendpunkten an die SIEM-Lösung zu übermitteln:

- Markieren Sie das Kästchen **Sicherheitstelemetrie**, um die Funktion zu aktivieren.
- Wählen Sie die SIEM-Lösung aus, mit der Sie die Verbindung herstellen möchten.
- Geben Sie die URL des SIEM-Servers an.

  Warnung
  HTTPS-Protokoll mit TLS 1.2 oder höher ist erforderlich. Andernfalls wird die Übermittlung von Ereignissen fehlschlagen.

- Geben Sie das Autorisierungstoken ein, das die Verbindung sichert.
- Legen Sie unter **Kommunikation zwischen Endpunkten und SIEMs** fest, ob Sie einen Proxy-Server verwenden möchten.

  Beachten Sie
  Der Agent verwendet für die Kommunikation mit dem SIEM den gleichen Proxy-Server wie für die Kommunikation mit GravityZone. Sie können die Einstellungen im Abschnitt **Allgemein > Einstellungen** einsehen.

Sobald die Richtlinie auf Endpunkte angewendet wird, beginnt der Agent mit der Übermittlung von auftretenden Ereignissen an den konfigurierten SIEM-Server.

7.2.2. 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.

  Scan bei Ausführung: Schützt proaktiv vor Bedrohungen und erkennt und blockiert automatisch dateilose Angriffe schon vor der Ausführung.
- 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.

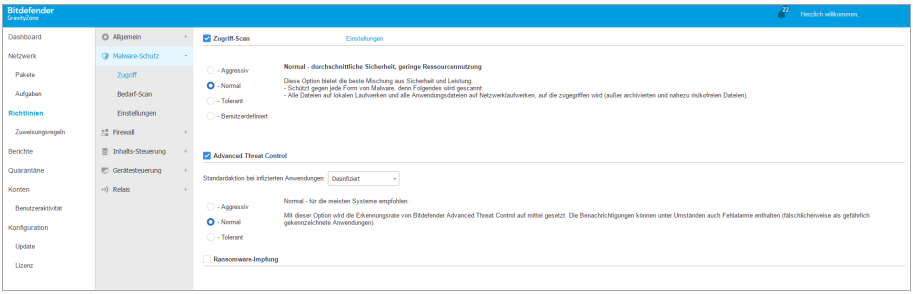
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- 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 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 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 im Kapitel „Anwendungsdateitypen“ (S. 483).

  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 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.

- **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 verbreiterter Ransomware-Varianten. Mit jedem Update der Sicherheitsinhalte werden neue Signaturen bereitgestellt, um auch neueste Bedrohungen zu neutralisieren.

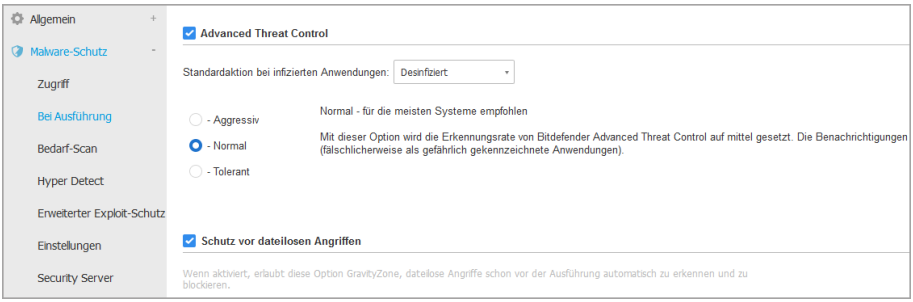
Warnung
Um noch besseren Schutz vor Ransomware-Infektionen zu gewährleisten, sollten Sie Vorsicht im Umgang mit unerwünschten und verdächtigen Anhängen walten lassen und sicherstellen,dass die Sicherheitsinhalte regelmäßig aktualisiert werden.

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:

- Cloud-basierte Bedrohungserkennung
- Advanced Threat Control
- Schutz vor dateilosen Angriffen
- Ransomware-Abhilfemaßnahme



Richtlinien - Einstellungen bei Ausführung

Advanced Threat Control

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 einen 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.

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.

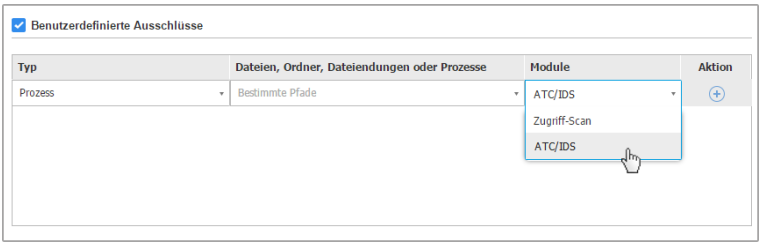
So konfigurieren Sie die Advanced Threat Control:

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 - ATC/IDS-Prozessauschluss

Schutz vor dateilosen Angriffen

Beachten Sie
Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

Der Schutz vor dateilosen Angriffen erkennt und blockiert dateilose Malware schon vor der Ausführung. Dazu gehört das Beenden der PowerShell bei Ausführung schädlicher Befehlszeilen, das Blockieren von schädlichem Datenverkehr, die Analyse des Arbeitsspeicherpuffers vor einer Code Injection und das Blockieren der eigentlichen Code Injection.

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**.

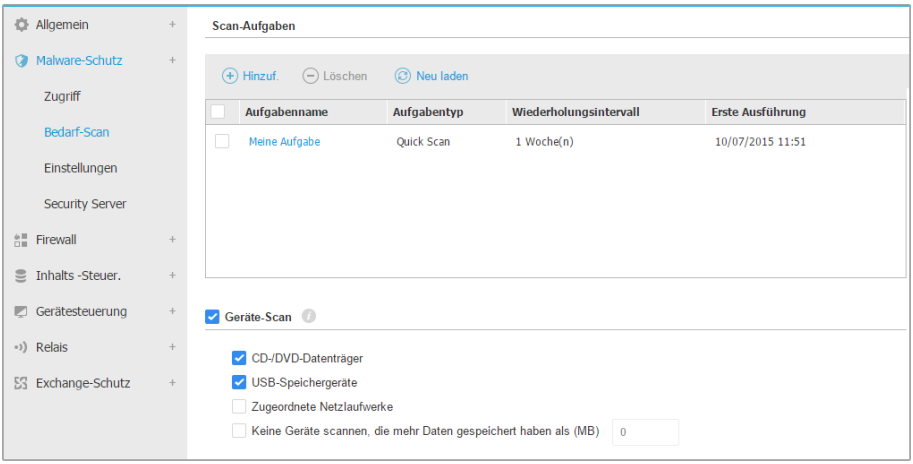
  Weitere Informationen zu dieser Benachrichtigung finden Sie unter „Benachrichtigungsarten“ (S. 460).
- Rufen Sie den Bericht **Sicherheitsüberprüfung** auf.
- Rufen Sie die Seite **Ransomware-Aktivität** auf.

  Weiter unten auf dieser Seite können Sie bei Bedarf Wiederherstellungsaufgaben starten. Weitere Informationen finden Sie im Kapitel ???.

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. 189).

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.



Richtlinien - 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 umgangen 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 Virenscan 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.

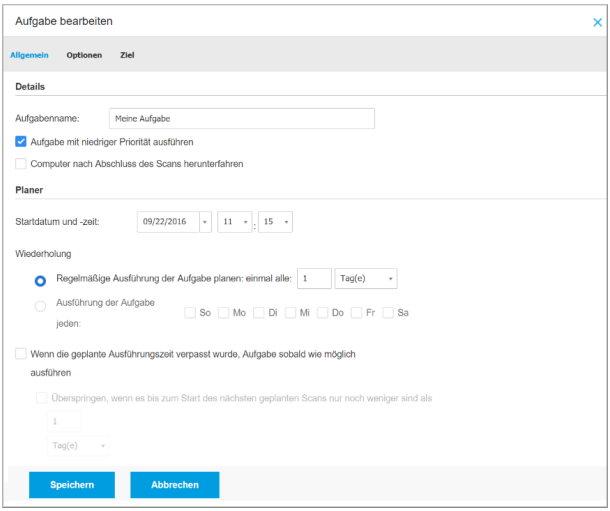
Um eine Aufgabe aus der Liste zu entfernen, klicken Sie auf die Schaltfläche ⊖ **Löschen** auf der rechten Seite der Tabelle.

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:



Richtlinien - 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 Zielendpunkts 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.

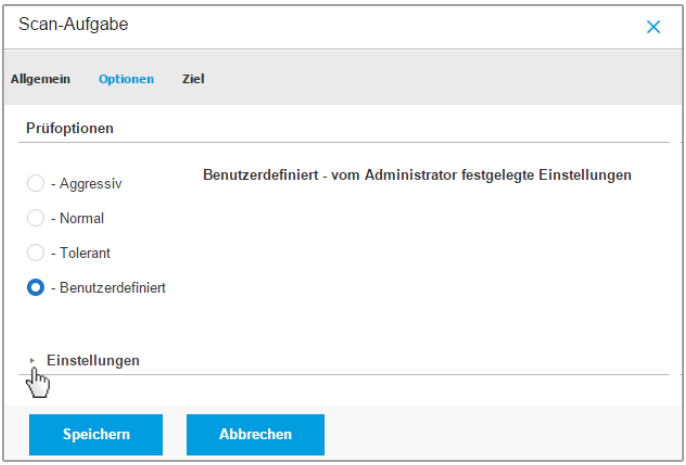
  Sie können optional festlegen, was passieren soll, wenn die Scan-Aufgabe nicht zur geplanten Zeit gestartet werden konnte (weil der Endpunkt offline oder ausgeschaltet war). Nutzen Sie bei Bedarf die Option **Wenn die geplante Ausführungszeit verpasst wird, Aufgabe so bald wie möglich ausführen**:

  – 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 - 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 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 im Kapitel „Anwendungsdateitypen“ (S. 483).

  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`.

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierten 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 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 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 verdächtigte 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.

- **Standardaktion für Rootkits.** Rootkits sind spezielle Software-Wekzeuge, 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 Menus 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 scann 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 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.

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. 189).

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 Klappmenü, 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 unbekannten 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. 184).

- **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. 185).

- **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. 185).

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 bösartige 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, bösartigen 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 bösartigem Code, über DLL-Exporte auf sensible Systemfunktionen zuzugreifen. Standardaktion: Prozess beenden
Shellcode Thread	Erkennt Versuche, bösartigen 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.

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 Objekttyen 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.

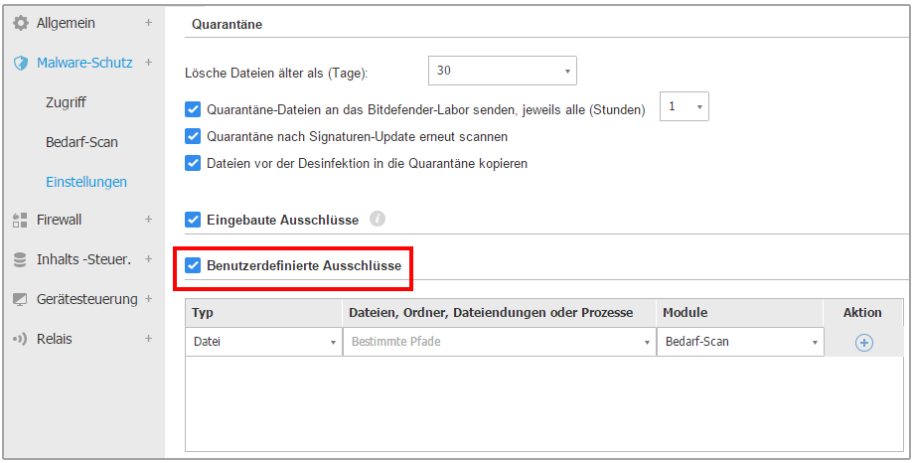
  Benutzerdefinierte Anti-Malware-Ausschlüsse gelten für eine oder mehrere der folgenden Scan-Methoden:

  – 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.



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 Dateiendung

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`.

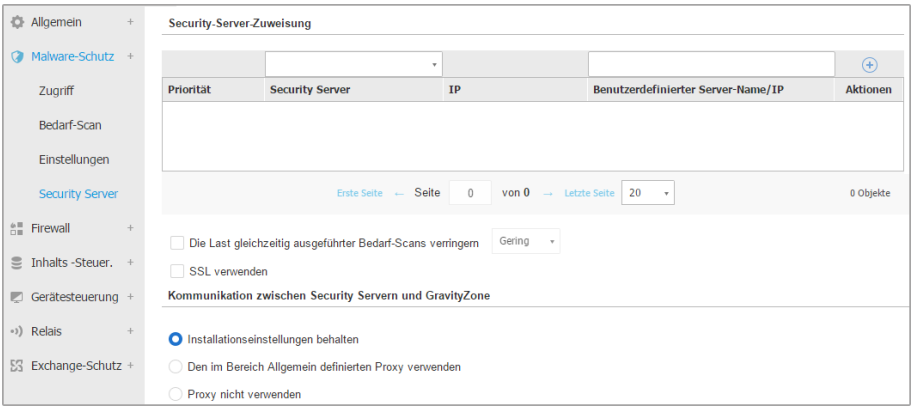
So importieren Sie benutzerdefinierte Ausschlüsse:

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. Weitere Details zum Thema Ports finden Sie im Artikel GravityZone-Kommunikationsports in der Wissensdatenbank.

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.

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 x MAX(b ; vCPUs - 1)`. Hierbei gilt:

   - `N` = Anzahl gleichzeitig erlaubter Scan-Aufgaben
   - `a` = Koeffizient mit folgenden Werten: `1` - für Gering; `2` - für Mittel; `4` - für Hoch
   - `MAX(b;vCPU-1)` = eine Funktion, die die Höchstzahl verfügbarer Scan-Slots auf dem Security Server zurückgibt.
   - `b` = die Standardanzahl an Bedarf-Scan-Slots (derzeit 4).
   - `vCPUs` = 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 x MAX(4 ; 12-1) = 4 x 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 ínstalliert ist.

- **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.

7.2.3. 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 die Sandbox Analyzer-Einstellungen für die automatische Übermittlung über Bitdefender Endpoint Security Tools konfigurieren. Informationen zur manuellen Übermittlung finden Sie unter „Manuelle Übermittlung“ (S. 453).

Endpunktsensor

Bitdefender Endpoint Security Tools kann auf Windows-Endpunkten als Einspeisungssensor für Sandbox Analyzer fungieren.

Richtlinien > Sandbox Analyzer > Endpunktsensor

Konfiguieren Sie den Sandbox Analyzer für die automatische Übermittlung:

1. **Verbindungseinstellungen**. Der Endpunktsensor ist so konfiguriert, dass Stichproben abhängig von Ihrem Standort an eine von Bitdefender gehostete Sandbox Analyzer-Standardinstanz übermittelt werden.
   - **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. 158).
   - 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. 486).

   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.

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. 244).

Beachten Sie
Ein Proxy, der in den Verbindungseinstellungen des Sandbox Analyzer konfiguriert wurde, setzt sämtliche Endpunkte mit Relais-Rolle außer Kraft.

7.2.4. 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. 207).

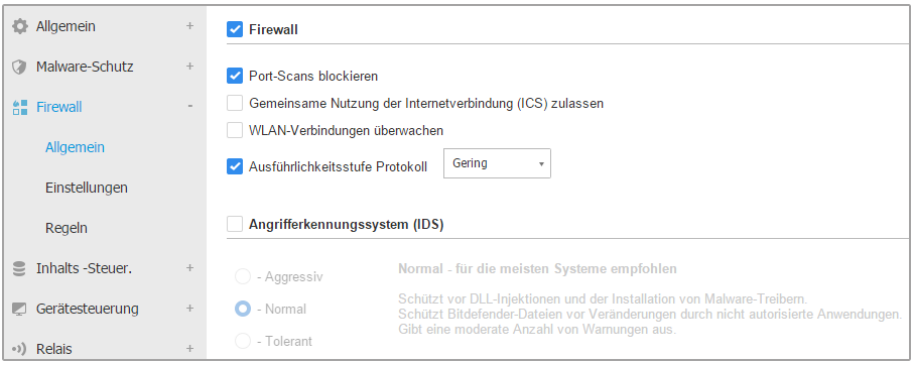
Wichtig
Das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

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.



- **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.

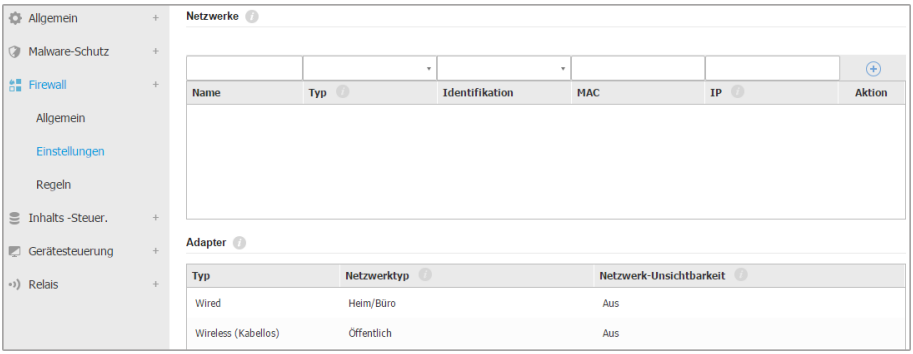
Wichtig
Das Angriffserkennungssystem ist nur für Endpoint Security-Clients verfügbar.

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



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.

Adaptereinstellungen

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.

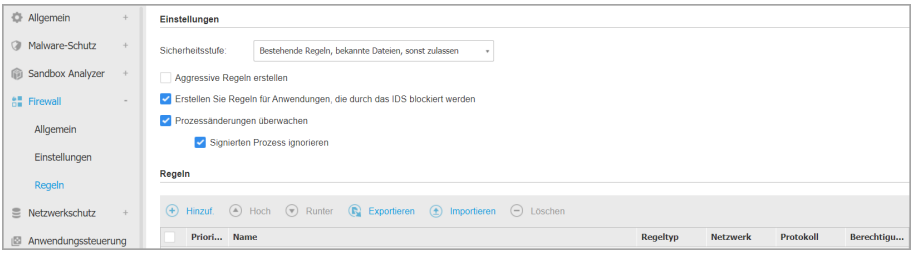
  Wenn die Erkennung auf der Basis des Windows-Netzwerkmanagers fehlschlägt, wird eine einfache Erkennung versucht. Ein generisches Profil wird angewendet, in dem das Netzwerkprofil **Öffentlich** zugrundegelegt und die Tarnkappeneinstellung auf **Ein** gestellt wird.

  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 - 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 unbekannten 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

unbekannten 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 unbekannten Verbindungsversuche zur Auswahl einer Aktion auffordern. Ein Warnfenster mit detaillierten Informationen über den unbekannten 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 Netzwerkkenntnisse 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.
- **Verbindungbasierte 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 vollständige Liste zugewiesener Nummern von IP-Protokollen finden Sie im Kapitel 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
`ruleType`	**Regeltyp**: 1 für **Anwendungsregel** 2 für **Verbindungsregel**
`Art`	Der Wert für dieses Feld ist optional.
`details.name`	**Name der Regel**
`details.applictionPath`	**Anwendungspfad** (nur für anwendungsbasierte Regeln)
`details.commandLine`	**Befehlszeile** (nur für anwendungsbasierte Regeln)
`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**

Feld	Name und Wert
	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
`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**

Feld	Name und Wert
	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.

7.2.5. 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 Identitätschutzregeln 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

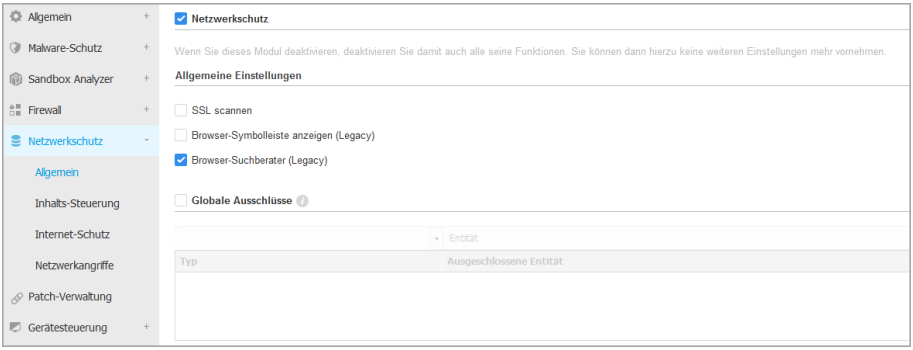
dazu in den Einstellungen unter **Sicherheit & Datenschutz** erteilen. Dieses Modul funktioniert erst, wenn der Benutzer der Bitdefender-Systemerweiterung zugestimmt hat. Bis dahin wird in der Endpoint Security for Mac-Benutzeroberfläche ein kritisches Problem angezeigt und die Zustimmung angefordert.
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 - 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-Symbolleiste anzeigen (Legacy)**. Die Bitdefender-Symbolleiste informiert Benutzer über die Bewertung der Webseiten, die sie aufrufen. Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. 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 Symbolleiste.

Abhängig davon, wie Bitdefender die Webseite einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste 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.
- Dieses 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.
- Dieses 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
`www.beispiel*`	Eine beliebige URL, die mit `www.Beispiel` beginnt (unabhängig von der Domainendung). Der Ausschluss gilt nicht für die Unterdomänen der angegebenen Website, so zum Beispiel `unterdomäne.beispiel.com`.
`*beispiel.com`	Jede URL, die mit `Beispiel.com` aufhört, einschließlich aller Subdomains.
`*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 Anwendungenimmer 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 Administrationen 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.

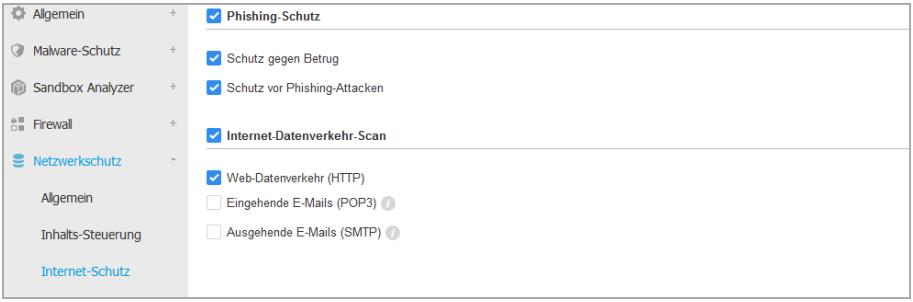
Beachten Sie
Wird eine E-Mail mit blockierten Inhalten an mehrere Empfänger adressiert, wird die Nachricht an die Empfänger verschickt, für die Ausschlüsse definiert wurden.

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 - 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.

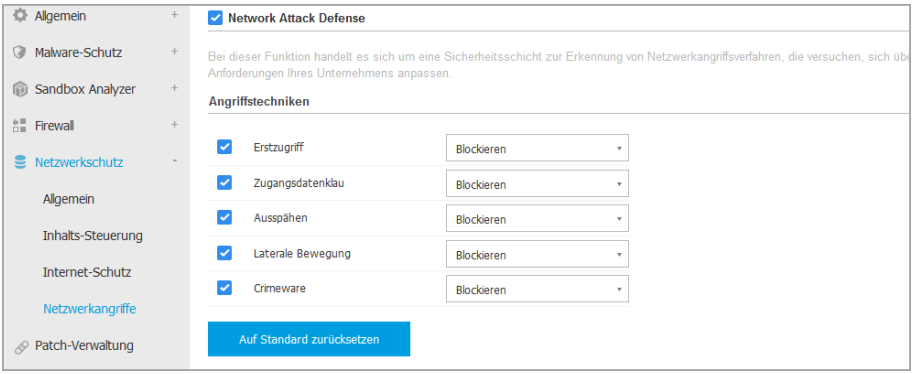
Wenn eine infizierte E-Mail erkannt wird, wird diese automatisch mit einer Standard-E-Mail ersetzt, die den Empfänger über die ursprüngliche infizierte E-Mail informiert. Wenn eine Webseite Malware enthält oder verbreitet, wird diese automatisch blockiert. Anstelle der Webseite wird eine Warnung angezeigt, die den Anwender darüber informiert, das 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.



Richtlinien - 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.

Beipiele: 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.

7.2.6. 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 herunterladen, 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

7.2.7. 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	
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.

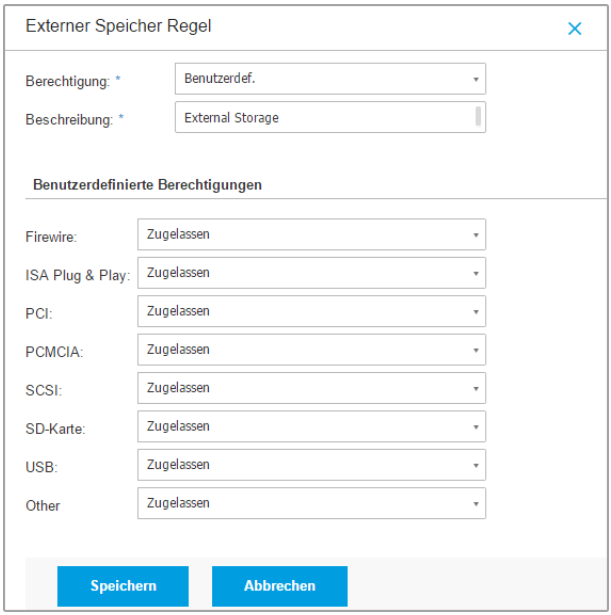
So legen Sie die Berechtigungen für einen bestimmten Gerätetyp fest:

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.



Richtlinien – 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**.

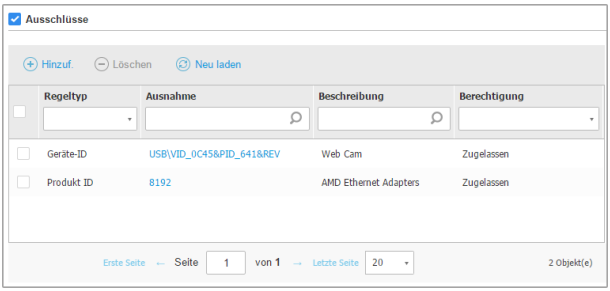
Wichtig

- 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.



Richtlinien - Gerätesteuerung - Ausschlüsse

7.2.8. 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.

- Der Standard-Update-Server für Relais-Agenten ist: http://upgrade.bitdefender.com. Sie können einen anderen Update-Server festlegen, indem Sie die IP-Adresse oder den lokalen Hostnamen einer oder

mehrerer Relais-Maschinen 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-Endpunkt 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 Udpate-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.

7.2.9. 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.

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 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.

Einstellungen

- **Quarantäne-Dateien löschen, die älter sind als (Tage).** Standardmäßig werden Dateien in der Quarantäne, die älter als 15 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 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:
  - **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 im Kapitel „Anwendungsdateitypen“ (S. 483).

    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 verdächtigte 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 vefügbar.
- 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:
  - **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 im Kapitel „Anwendungsdateitypen“ (S. 483).

    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**. 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 verdächtigte 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.
- **Realtime 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 unbekannten 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. 263)
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. 261).

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. 266)

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 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 Nachrichteninhalt 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. 267).

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 welchen 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 sprechenden Tabelle enthält, werden gefiltert.
     - Im Nachrichteninhalt. Markieren Sie dazu das Kästchen **Nach Nachrichteninhalt filtern**. Alle E-Mails, die im Nachrichteninhalt 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 Nachrichteninhalt 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 Vierergrupppen 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 `Lotterie`, `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 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 vertrauenswürdig 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 Anhangangsfilterung 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. 267).

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. 484).

     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 Archivtiefe (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 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 vertrauenswürdig sind**.
4. Klicken Sie auf **Speichern**.

7.2.10. 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.

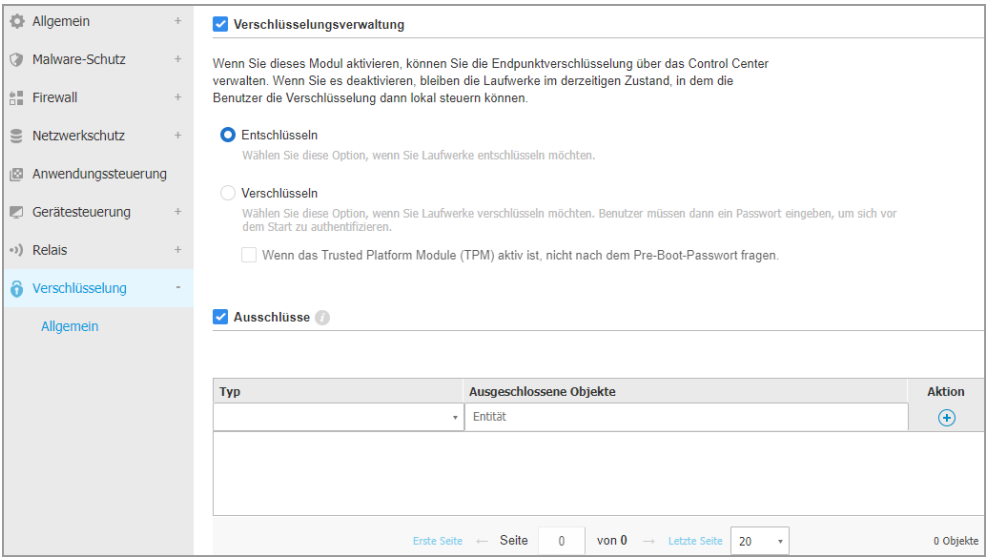
Durch diesen Ansatz bietet GravityZone einige attraktive Vorteile:

- 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.



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. 281).

- **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. 117).

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.
   - Als **GUID** geben Sie 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** ⊗.

7.2.11. 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

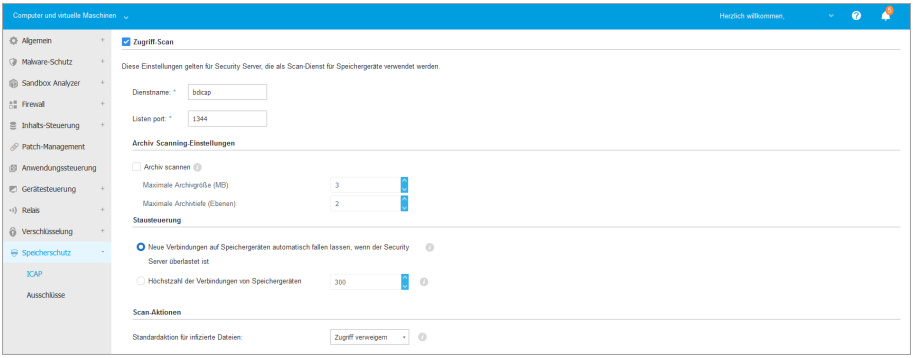
ICAP

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
```

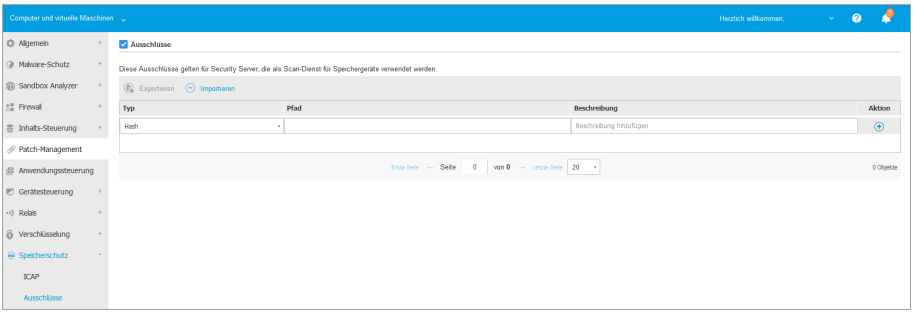
So können Sie Ausschlüsse importieren:

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`.

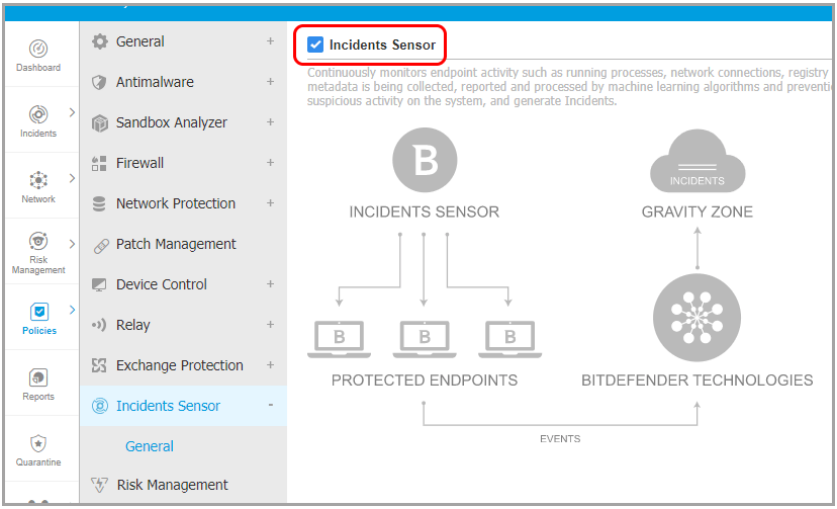


Richtlinien- Speicherschutz - ICAP

7.2.12. Vorfallsensor

Der Vorfallsensor überwacht kontinuierlich Endpunktaktivitäten wie laufende Prozesse, Netzwerkverbindungen, Registrierungsänderungen und Benutzerverhalten. Diese Metadaten werden von maschinellen Lernenalgorithmen und Präventionstechnologien erfasst, gemeldet und verarbeitet, die verdächtige Aktivitäten auf dem System erkennen und Vorfälle erzeugen.

Markieren Sie das Kästchen Vorfallsensor, um dieses Modul zu aktivieren.



Vorfallsensor

7.2.13. Risiko-Management

Beachten Sie
Dieses Modul ist verfügbar für:

- Windows für Workstations
- Windows für Server

Das Modul für die Endpunkt-Risikoanalyse hilft Ihnen, eine Vielzahl von Netzwerk- und Betriebssystemrisiken auf Endpunktebene zu identifizieren und zu beheben. Dies erfolgt über Risiko-Scan-Aufgaben, die über Richtlinien zur wiederkehrenden Ausführung auf den Zielendpunkten konfiguriert werden können.

Ihnen steht eine umfangreiche Liste mit Risikoindikatoren zur Auswahl, um Ihre Endpunkte zu scannen und festzustellen, ob sie angreifbar sind. Weitere Informationen zu den Risikoindikatoren in GravityZone finden Sie in diesem Artikel in der Wissensdatenbank.

So können Sie die Endpunkt-Risikoanalyse konfigurieren:

- Markieren Sie das Kästchen, um die **Risiko-Management**-Funktionen zu aktivieren. Sie können dann Richtlinien erstellen, die festlegen, wie **Risiko-Scan**-Aufgaben durchgeführt werden.
- **Planer**: Legen Sie einen Zeitplan für die Risiko-Scans auf den Zielendpunkten fest:
  1. Geben Sie das Startdatum und die Startzeit für den geplanten Risiko-Scan an.
  2. Legen Sie den Scan-Wiederholungstyp fest:
     - Regelmäßig, nach der angegebenen Anzahl von Stunden / Tagen / Wochen.
     - Nach Wochentag.

Wichtig
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.

Der geplante Scan wird zur lokalen Zeit des Zielendpunkts 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.

3. 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.

Risiko-Scan-Aufgaben werden für alle standardmäßig aktivierten Risikoindikatoren ausgeführt.

Nachdem ein Risiko-Scan-Aufgabe erfolgreich abgeschlossen wurde, können Sie diese Indikatoren im Reiter Fehlkonfigurationen auf der Seite **Sicherheitsrisiken** analysieren und ggf. auswählen, welche Indikatoren ignoriert werden sollen.

Der allgemeine Risikobewertung des Unternehmens wird auf Grundlage der ignorierten Risikoindikatoren erneut berechnet.

Beachten Sie
Die vollständige Liste der Risiko-Indikatoren und deren Beschreibung finden Sie in diesem Artikel in der Wissensdatenbank.

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.

Der GravityZone-Überwachungsabschnitt besteht aus:

- **Dashboard**
- **Executive Summary**

8.1. Dashboard

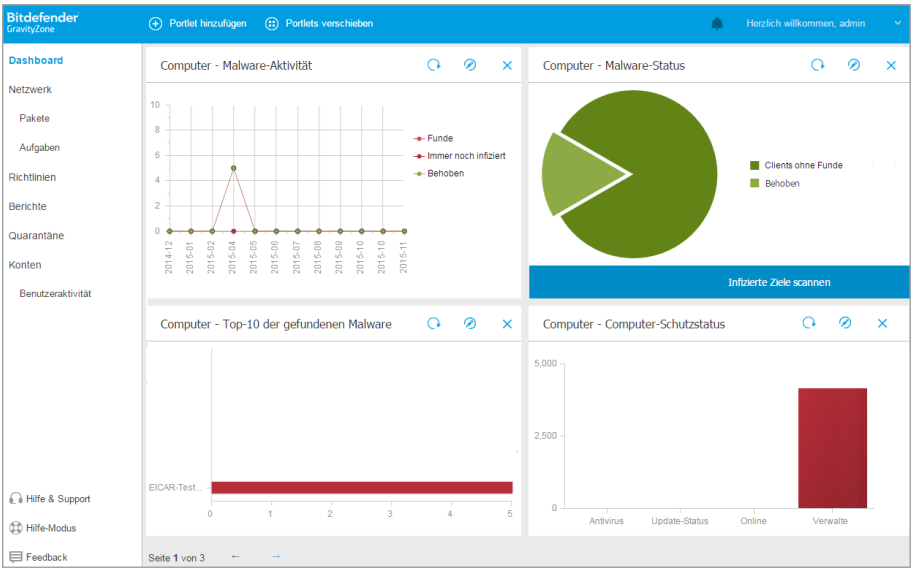
Das Control Center-Dashboard ist eine individuell anpassbare Oberfläche, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Endpunkte und den Netzwerkstatus verschafft.

Es besteht aus zwei Bereichen:

- Dashboard-Netzwerkstatusleiste
- Dashboard-Portlets

Die Dashboard-Netzwerkstatusleiste hält Sie über die Anzahl der offenen oder laufenden Vorfälle, bedrohten Assets (Endpunkte) und erkannte Bedrohungen in Ihrem Netzwerk auf dem Laufenden. Nutzen Sie diese Informationen, um nicht behobene Netzwerkobjekte zu überfliegen. Klicken Sie auf **Ansicht**, um die Seite **Vorfälle** aufzurufen. Weitere Informationen finden Sie unter „Vorfälle untersuchen“ (S. 299).

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 Berichttypen 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:

- Art des Hintergrundberichts
- Aussagekräftiger Portlet-Name
- Das Intervall, in dem die Ereignisse berichtet werden

Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter „Berichtstypen“ (S. 410).

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:

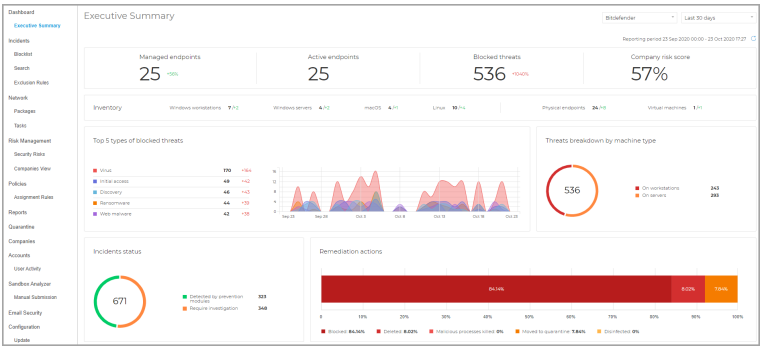
1. Gehen Sie zur Seite **Dashboard**.
2. Ziehen Sie die einzelnen Portlets mit der Maus an die gewünschte Stelle. Alle anderen Portlets zwischen der alten und der neuen Position behalten ihre Anordnung bei.

> **Beachten Sie**
> Sie können Portlets nur innerhalb der bestehenden Positionen verschieben.

8.2. Executive Summary

Executive Summary bietet einen kompakten Sicherheitsüberblick über alle geschützten Endpunkte in Ihrem Netzwerk und wurde speziell entwickelt, um Ihnen bei der Überwachung und Analyse zu helfen und der Unternehmensleitung aufschlussreiche Informationen zur Verfügung zu stellen.

Die Executive Summary besteht hauptsächlich aus Widgets und sorgt mit Details zu Endpunktmodulen, Funden und ergriffenen Maßnahmen, Bedrohungsarten und -techniken, Risikobewertung des Unternehmens und vielem mehr für einen transparenten Sicherheitsbetrieb.



Executive Summary

Wichtig

- Alle bereitgestellten Statistiken basieren auf Daten, die nach der Aktivierung der Funktion gesammelt wurden. Es werden keine früheren Ereignisse berücksichtigt.

Oben auf der Seite finden Sie die folgenden ersten Abschnitte:

Verwaltete Endpunkte
In diesem Abschnitt werden alle Maschinen in Ihrem Netzwerk aufgeführt, auf denen der Sicherheitsagent installiert ist.

Aktive Endpunkte
In diesem Abschnitt finden Sie alle Endpunkte, die im ausgewählten Zeitraum online waren oder zum Zeitpunkt der Berichterstattung online sind.

Blockierte Bedrohungen
Dieser Abschnitt zeigt die Gesamtzahl der blockierten Bedrohungen, die auf Ihren Endpunkten identifiziert wurden.

Inventar
Dieser Abschnitt enthält Einzelheiten zu den Endpunkttypen und ihren Betriebssystemen.

Risikobewertung des Unternehmens
In diesem Abschnitt finden Sie Informationen zur Risikobewertung Ihres Unternehmens.

Oben rechts auf der Seite können Sie den Namen eines Unternehmens eingeben oder aus dem Dropdown-Menü das gewünschte Unternehmen auswählen. Bitte

beachten Sie, dass die Zusammenfassung Statistiken für jeweils ein einzelnes Unternehmen und nicht für die gesamte Baumstruktur liefert.

Sie können auch einen vordefinierten Zeitraum (relativ zum aktuellen Datum) auswählen:

- **Letzte 24 Stunden**
- **Letzte 7 Tage**
- **Letzte 30 Tage**

Beachten Sie

- Alle präsentierten Daten sind direkt mit der ausgewählten Periode und dem Unternehmen korreliert.
- Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie oben rechts in der Tabelle auf **Neu laden**.

Je nach ausgewähltem Intervall kann es vorkommen, dass in einigen Abschnitten eine Differenz (Delta) in Prozent angezeigt wird.

Deltawerte zeigen die Unterschiede in Ihrem Netzwerk an, die zwischen zwei bestimmten Zeiträumen aufgetreten sind:

- Der Zeitraum vor dem ausgewählten Intervall mit der gleichen Anzahl an Tagen oder Stunden.
- Das ausgewählte Intervall.

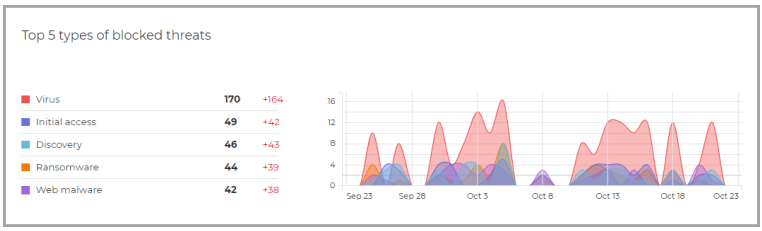
In der Abbildung unten ist beispielsweise die Gesamtzahl der blockierten Bedrohungen in Ihrem Netzwerk in den **Letzten 30 Tagen** um **6 %** gesunken. Diese Prozentzahl ergibt sich aus dem Vergleich der Werte aus den 30 Tagen vor dem ausgewählten Intervall mit den Werten aus den letzten 30 Tagen.

Executive Summary - Delta

Dies sind die wichtigsten Widgets in der Summary:

Top 5 der blockierten Bedrohungen

Das Widget gibt anhand der Anzahl der Funde an Ihren Endpunkten Auskunft über die häufigsten Bedrohungsarten. In der linken Spalte werden die Bedrohungstypen angezeigt und in der rechten Spalte finden Sie korreliert die Anzahl der Entdeckungen für jeden Typ sowie Delta-Werte.



Executive Summary - Top 5 der blockierten Bedrohungstypen

Aufschlüsselung der Bedrohungen nach Maschinentyp

Dieses Widget zeigt die Typen von Endpunkten, Arbeitsplatzrechnern und Servern sowie die jeweilige Anzahl von Funden.

Vorfallstatus

Dieses Widget enthält Einzelheiten zu den Sicherheitsvorfällen im gesamten Unternehmensnetzwerk.

Die Vorfallkategorien werden wie folgt beschrieben:

- **Entdeckt durch Präventionsmodule**: Sicherheitsereignisse, die von den GravityZone-Präventionsmodulen als Bedrohungen identifiziert wurden.
- **Erfordern Untersuchung**: verdächtige Vorfälle an, die eine Untersuchung erfordern und bei denen noch keine Maßnahmen ergriffen wurden.

Bereinigungsaktionen

In diesem Abschnitt werden die Aktionen beschrieben, die auf der Grundlage der angewandten Richtlinieneinstellungen bei blockierten Objekten durchgeführt wurden.

Status der Endpunktmodule

Ermöglicht einen Überblick über die Abdeckung durch Sicherheitsmodule auf Ihren Endpunkten. Das Diagramm zeigt die Module und gibt an, ob sie auf Ihren Endgeräten aktiviert, deaktiviert oder nicht installiert sind.

Risikobewertung des Unternehmens

In diesem Widget finden Sie Informationen zum Grad des Risikos, dem Ihr Unternehmen durch falsch konfigurierte Systemeinstellungen, bekannte Schwachstellen in den aktuell installierten Anwendungen und möglicherweise durch Benutzeraktivitäten und -verhalten hervorgerufene Risiken ausgesetzt ist.

Funde aufgrund von Richtlinienregeln

Dieser Abschnitt gibt Aufschluss über die Anzahl der Funde und den Typ der Funde auf Grundlage der Regeln, die vom Administrator in der Richtlinie festgelegt wurden.

Die Fundtypen umfassen:

- **Blockierte Geräte**: die Anzahl der Funde auf Grundlage der Regeln der **Gerätesteuerung**.
- **Blockierte Verbindungen**: die Anzahl der Funde auf Grundlage der **Firewall**-Regeln.
- **Blockierte Anwendungen**: die Anzahl der Funde auf Grundlage der Regeln der **Anwendungs-Blacklist**.
- **Blockierte Websites**: die Anzahl der Funde auf Grundlage der Regeln der **Internet-Zugangssteuerung**.

Blockierte Websites

Dieses Widget zeigt die Anzahl der Funde geordnet nach Bedrohungstyp, die auf Ihren Endpunkten durch den **Netzwerkschutz** gefunden wurden.

Blockierte Netzwerkangriffsverfahren

In diesem Abschnitt finden Sie Informationen über die blockierten Angriffstechniken, die in Ihrem Netzwerk gefunden wurden.

9. VORFÄLLE UNTERSUCHEN

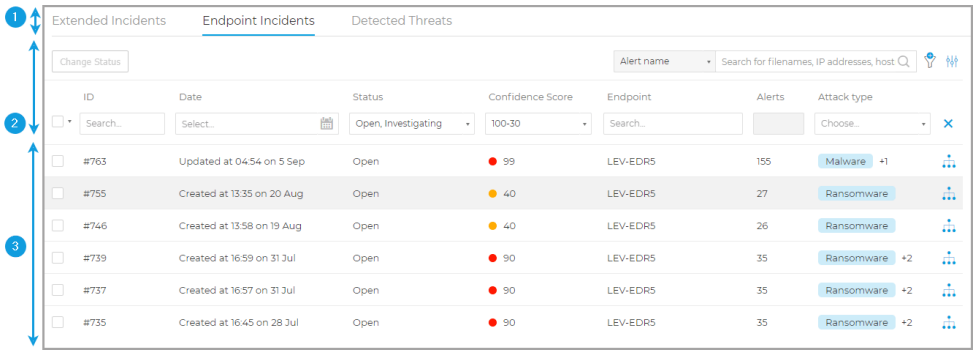
Im Bereich **Vorfälle** können Sie alle vom Vorfall-Sensor während eines bestimmten Zeitraums gemeldeten Sicherheitsereignisse untersuchen, filtern und entsprechende Bereinigungsaktionen durchführen.

Der Abschnitt **Vorfälle** umfasst die folgenden Seiten:

- **Vorfälle**: zur Anzeige und Untersuchung von Sicherheitsereignissen.
- **Blockierliste**: zur Verwaltung blockierter Dateien, die an Sicherheitsereignissen beteiligt waren.
- **Suche**: zur Auswahl von Optionen für Abfragen der Datenbank der Sicherheitsereignisse.

9.1. Die Vorfallsseite

Auf der Seite **Vorfälle** können Sie Sicherheitsereignisse filtern und verwalten.



Vorfallsübersicht

Beachten Sie
Die Verfügbarkeit dieser Reiter hängt von der in Ihrem aktuellen Abonnementplan enthaltenen Lizenz ab.

Diese Seite umfasst die folgenden Bereiche:

1. Eine Fensterleiste mit Reitern, die verschiedene Ereignistypen enthalten:

- **Endpunktvorfälle**: zeigt alle verdächtigen Vorfälle an, die auf Endpunktebene gefunden wurden, die eine Untersuchung erfordern und für die noch keine Maßnahmen ergriffen wurden.
- **Gefundene Bedrohungen**: zeigt Sicherheitsereignisse, die von den GravityZone-Präventionsmodulen als Bedrohungen identifiziert wurden. Diese Vorfälle werden auf Endpunktebene gefunden und mit Maßnahmen behandelt, die in den auf Ihre Umgebung angewendeten Sicherheitsrichtlinien vordefiniert sind.

2. Filteroptionen zur individuellen Anpassung Ihres Rasters:
   - Über die Schaltfläche **Spalten ein-/ausblenden** können Sie einzelne Filterspalten hinzufügen oder entfernen.

     Die Seite wird automatisch mit den Karten der Sicherheitsereignisse neu geladen, deren Daten zu den hinzugefügten Filterspalten passen.
   - Über die Schaltfläche **Filter ein-/ausblenden** können Sie die Filterleiste ein- oder ausblenden.
   - Über die Schaltfläche **Filter löschen** können Sie alle Filter auf den Ausgangszustand zurücksetzen.
3. Das Raster Vorfälle, das eine Liste der Sicherheitsereignisse anzeigt, die den ausgewählten Filtern entsprechen.

Beachten Sie
Diese Funktion unterstützt nicht mehr den Internet Explorer.

Die Übersichtsleiste

In der Leiste **Übersicht** finden Sie offene Vorfälle, häufigste Warnmeldungen, betroffene Geräte und andere relevante Daten, um Ihnen einen schnellen Überblick über die allgemeine Bedrohungslage in Ihrer Umgebung zu geben.

Die Übersichtsleiste

Beachten Sie
Die Verfügbarkeit und der Inhalt der Leiste **Übersicht** hängt von der in Ihrem aktuellen Abonnementplan enthaltenen Lizenz ab.

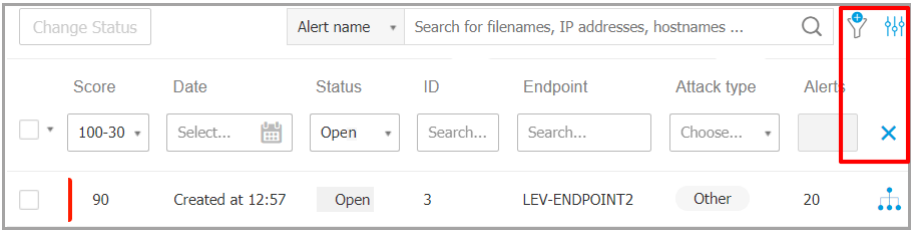
Vorfälle in der Übersichtsleiste filtern

Sie können die Vorfallliste filtern, indem Sie einzelne Werte in der Übersichtsleiste auswählen:

- Wenn Sie auf einen Wert im Bereich **OFFENE VORFÄLLE** klicken, werden nur die Vorfälle angezeigt, die den ausgewählten Schweregrad haben.
- Wenn Sie im Bereich **HÄUFIGSTE WARNMELDUNGEN** auf einen Wert klicken, wird der Name der Warnmeldung ins Suchfeld eingefügt und es werden nur die Vorfälle angezeigt, bei denen diese Warnmeldung ausgegeben wurde.
- Wenn Sie im Bereich **HÄUFIGSTE TECHNIKEN** auf einen Wert klicken, wird der Name der Technik ins Suchfeld eingefügt und es werden nur die Vorfälle angezeigt, bei denen diese Technik angewendet wurde.
- Wenn Sie im Bereich **AM HÄUFIGSTEN BETROFFENE GERÄTE** auf einen Wert klicken, werden nur die Vorfälle angezeigt, die das gewählte Gerät betreffen.

9.1.1. Die Filterleiste

Auf der Seite **Vorfälle** können Sie über eine Vielzahl von Filtern festlegen, welche Ereignisse angezeigt werden.



Die Filterleiste

- Über die Schaltfläche **Spalten ein-/ausblenden** können Sie einzelne Filterspalten hinzufügen oder entfernen.

  Die Seite wird automatisch mit den Karten der Sicherheitsereignisse neu geladen, deren Daten zu den hinzugefügten Filterspalten passen.

- Über die Schaltfläche **Filter ein-/ausblenden** können Sie die Filterleiste ein- oder ausblenden.
- Über die Schaltfläche **Filter löschen** können Sie alle Filter auf den Ausgangszustand zurücksetzen.

Die verfügbaren Filter werden in der folgenden Tabelle im Detail beschrieben:

Filterungsoptionen	Details
Anzahl	Der Konfidenzwert ist eine Zahl zwischen 10 und 100, mit der dargestellt werden soll, wie potenziell gefährlich ein Sicherheitsereignis ist. Je höher der Wert, desto wahrscheinlicher ist es, dass das Ereignis gefährlich ist. Er errechnet sich aus Angriffsindikatoren und/oder ATT&CK-Techniken. Sie können nach Konfidenzwert filtern, indem Sie den Schieberegler auf die gewünschten Werte schieben. Sie können die gewünschten Werte auch in die Felder unter dem Schieberegler eingeben. Klicken Sie auf **OK**, um die Auswahl der Werte zu bestätigen.
Datum	Gehen Sie folgendermaßen vor, um nach dem Datum zu filtern: 1. Klicken Sie auf das Kalendersymbol oder das **Datumsfeld**, um die Datumskonfigurationsseite zu öffnen. 2. Wählen Sie den Zeitraum, in dem der Vorfall auftrat: • Klicken Sie auf die Schaltflächen **Von** und **Bis**, um Beginn und Ende des Zeitraums festzulegen. **Beachten Sie** Über die Felder für Stunden und Minuten können Sie den genauen Zeitpunkt für den Beginn und das Ende des gewünschten Zeitraums eingeben. • Sie können auch einen vordefinierten Zeitraum (relativ zum aktuellen Datum) auswählen (Für die letzten 7 Tage. Um zusätzlichen Speicherplatz für Ereignisse zu erhalten, wenden Sie sich bitte an Ihren zuständigen Vertriebsmitarbeiter, um Ihre Lösung mit einem Add-on

Filterungsoptionen	Details
	für 30, 90 oder 180 Tage **Datenspeicherung** zu erweitern). 3. Klicken Sie auf **OK** um den Filter anzuwenden.
Status	Im **Status**-Klappmenü können Sie einen oder mehrere Status auswählen, um nur Ereignisse mit diesem/diesen Status anzuzeigen: • **Offen**: für noch nicht untersuchte Sicherheitsereignisse • **Untersuchung läuft**: für Sicherheitsereignisse, die derzeit untersucht werden • **Fehlalarm**: für Sicherheitsereignisse, die als Fehlalarm gekennzeichnet wurden. • **Abgeschlossen**: für Sicherheitsereignisse, deren Untersuchung abgeschlossen wurde
ID	Im Feld ID können Sie eine konkrete Sicherheitsereignis-ID eingeben, um nur Karten anzuzeigen, die dieser ID zugeordnet sind.
Endpunkt	Im Feld Endpunkt können Sie den Namen eines Endpunkts innerhalb Ihres Netzwerks eingeben, um nur die Karten anzuzeigen, die diesem Endpunkt zugeordnet sind.
Angriffstyp	Unter Angriffstyp findet sich eine dynamische Liste der häufigsten Angriffstypen, die je nach den Angriffsindikatoren in den aufgeführten Sicherheitsereignissen andere Einträge enthält.
Warnmeldungen	In der Spalte **Warnmeldungen** wird die Anzahl der ausgelösten Warnmeldungen pro Vorfall angezeigt.
Endpunkt-BS	Hiermit können Sie die Sicherheitsereignisse nach den Betriebssystemen der betroffenen Endpunkte filtern.

Beachten Sie
Die verfügbaren Filteroptionen hängt von der in Ihrem aktuellen Abonnementplan enthaltenen Lizenzschlüssel ab.

Nach Elementen, die zunächst nicht in der Filterleiste angezeigt werden, können Sie über das Eingabefeld **Suche** und das daneben angezeigte Klappmenü suchen:

- **Name der Warnmeldung** - 3 bis 1000 Zeichen
- **ATT&CK-Technik** - bis zu 100 Zeichen
- **Endpunkt-IP** - bis zu 45 Zeichen
- **MD5** - bis zu 32 Zeichen
- **SHA256** - bis zu 64 Zeichen
- **Knotenname** - bis zu 360 Zeichen
- **Benutzername** - bis zu 1000 Zeichen

Die Seite wird automatisch neu geladen und nur die Karten der Sicherheitsereignisse angezeigt, die zum gesuchten Element passen. Detailliertere Suchen können Sie auf der Suchseite durchführen.

9.1.2. Liste der Sicherheitsereignisse anzeigen

Auf der Seite **Vorfälle** wird eine Liste der Sicherheitsereignisse angezeigt, die den ausgewählten Filtern entsprechen.

Standardmäßig werden 20 Ereignisse pro Seite angezeigt, gebündelt nach Datum. In regelmäßigen Abständen wird die Seite neu geladen und dann etwaige neu erkannte Ereignisse angezeigt.

Wichtig
Alle Sicherheitsereignisse, die älter als 90 Tage sind, werden sowohl aus den Abschnitten **Endpunktvorfälle** und **Gefundene Bedrohungen** als auch aus dem Repository für Sicherheitsereignisse automatisch gelöscht.

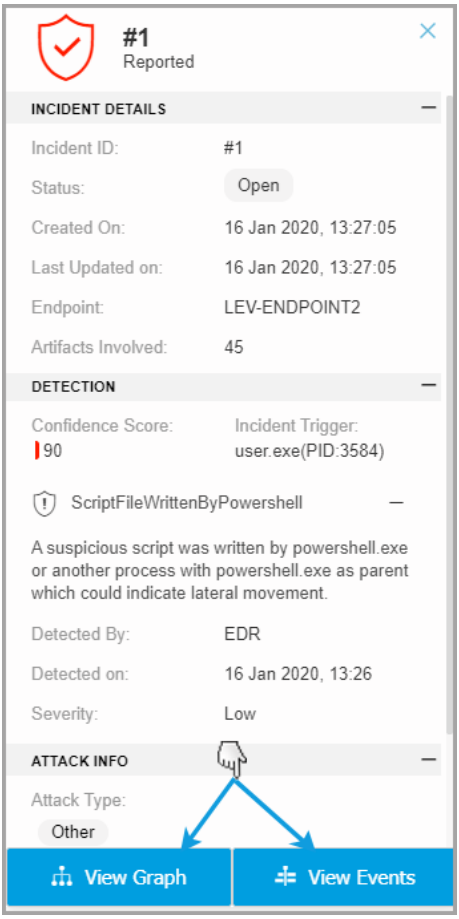
Die Seite hoch und runter scrollen können Sie mithilfe der Pfeiltasten, des Mausrads oder der Scroll-Leiste. Sie können unten auf der Seite die Anzahl der angezeigten Ereignisse anpassen. Sie können bis zu 100 Ereignisse pro Seite anzeigen.

Jedes Sicherheitsereignis wird als Rich Card dargestellt, auf der je nach den eingestellten Filtern die relevanten Informationen zu diesem Ereignis angezeigt werden.

Beachten Sie
Anhand der Farbe am linken Rand, können Sie den Konfidenzstufe (niedrig, mittel oder hoch) schnell beurteilen.

Sicherheitsereigniskarte

- Wenn Sie auf die Schaltfläche **Diagramm anzeigen** einer Ereigniskarte klicken, wird dieses Ereignis in einer neue Seite geöffnet, auf der Sie weitere Details zu diesem Ereignis sehen und die nötigen Aktionen durchführen können.
- Wenn Sie an einer anderen Stelle auf eine Sicherheitsereigniskarte klicken, wird ein Übersichtsfenster an der Seite angezeigt, auf dem ebenfalls weitere Details zu dem Ereignis stehen.



Schnellansicht der Details zu einem Vorfall

  - Wenn Sie hier auf die Schaltfläche **Diagramm anzeigen** klicken, wird eine graphische Darstellung des Vorfalls angezeigt.
  - Wenn Sie auf die Schaltfläche **Ereignisse anzeigen** klicken, wird die Zeitleiste des Vorfalls angezeigt.

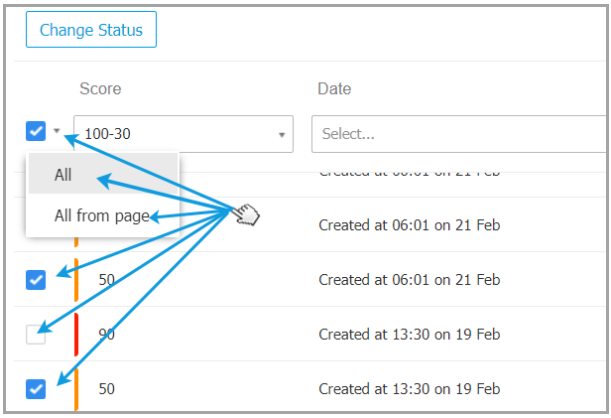
- Wenn Sie das Kästchen einer Sicherheitsereigniskarte markieren, wird die Schaltfläche **Status ändern** aktiviert, über die Sie den Status des Vorfalls ändern können.

Ändern des Status von Sicherheitsereignissen

Mit dem Untersuchungsstatus behalten Sie den Überblick über bereits untersuchte und als abgeschlossen oder Fehlalarm markierte Vorfälle, derzeit untersuchte Vorfälle sowie offene oder neue Vorfälle, die noch nicht analysiert wurden.

Sie können den Status eines oder mehrerer Sicherheitsereignisse gleichzeitig ändern:

1. Markieren Sie die Kästchen aller Vorfälle, deren Status Sie ändern möchten.

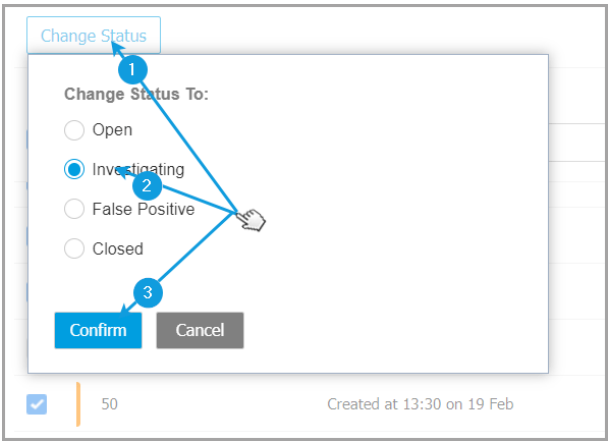


Sicherheitsereigniskarten markieren

Sie können die gewünschten Karten einzeln auswählen oder über die Auswahloptionen im Klappmenü mehrere gleichzeitig auswählen.

Beachten Sie
Auch wenn Sie durch mehrere Seiten mit Sicherheitsereignissen blättern, bleibt Ihre Auswahl bestehen.

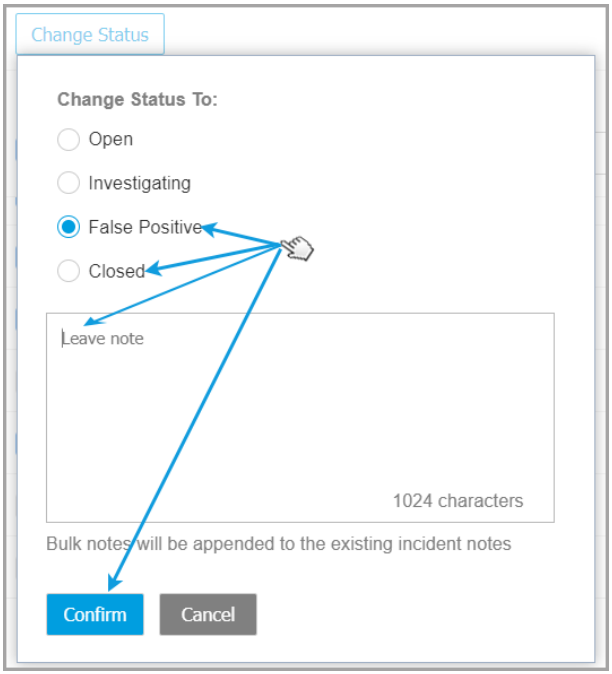
2. Klicken Sie auf die Schaltfläche **Status ändern** und wählen Sie die gewünschte Option:



Ändern des Status von Sicherheitsereignissen

- **Offen** - Wenn das Sicherheitsereignis bisher noch nicht untersucht wurde.
- **Untersuchung läuft** - Wenn Sie bereits angefangen haben, das Ereignis zu untersuchen.
- **Fehlalarm** - Wenn Sie das Ereignis analysiert und als Fehlalarm identifiziert haben.
- **Abgeschlossen** - Wenn Sie die Untersuchung des Ereignisses abgeschlossen haben.

> **Beachten Sie**
> Wenn Sie den Status eines oder mehrerer Ereignisse auf **Fehlalarm** oder **Abgeschlossen** setzen, wird ein Eingabefeld angezeigt, in dem Sie die Gründe für die Statusänderung oder andere Notizen eingeben können.



Notiz anfügen, wenn der Status auf Fehlalarm oder Abgeschlossen gesetzt wird

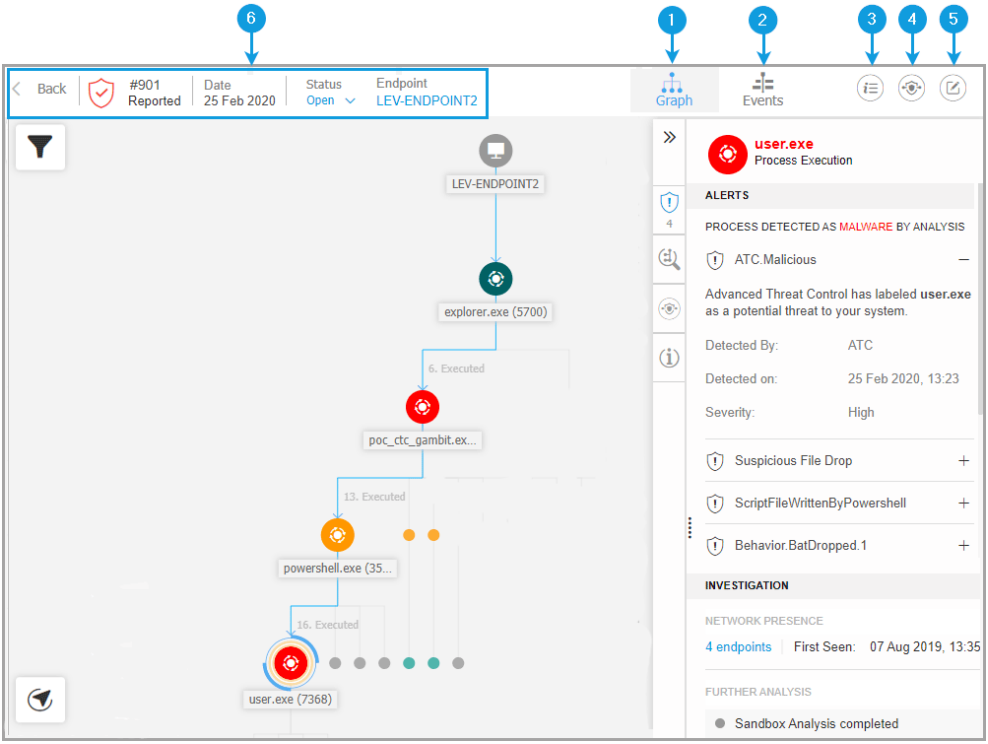
Beachten Sie
Die Notiz wird zu evtl. schon bestehenden hinzugefügt.

3. Klicken Sie auf **Bestätigen**, um die ausgewählte Statusoption anzuwenden.

9.1.3. Untersuchen eines Endpunktvorfalls

Klicken Sie auf der Seite **Vorfälle** auf die Schaltfläche **Diagramm anzeigen** des Sicherheitsereignisses, das Sie untersuchen möchten. Es wird eine neue Seite mit Detailinformationen zu diesem Ereignis geöffnet.

Für jeden Sicherheitsvorfall gibt es eine eigene Seite mit detaillierten Informationen zur Abfolge der Ereignisse (im Diagramm als verbundene Sicherheitsereignisknoten angezeigt), die zur Auslösung des Vorfalls geführt haben, und bietet Optionen zur Bereinigung.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Diagrammreiter

   Das Diagramm zeigt den Sicherheitsvorfall und die dazugehörigen Elemente an, wobei der kritische Pfad des Vorfalls hervorgehoben wird und die Details des Knotens, der den Vorfall ausgelöst hat, im Bereich **Knotendetails** angezeigt werden.

2. Ereignisreiter

   Im Reiter Ereignisse werden filterbare erkannte Systemereignisse und Warnmeldungen sowie die entsprechenden Ereignisbeschreibungen angezeigt.

3. Vorfallsinformationen

   In diesem Bereich finden Sie reduzierbare Abschnitte mit Details wie Vorfalls-ID, aktueller Status, Zeitstempel der Erstellung und letzten Aktualisierung, Anzahl der beteiligten Artefakte, Name des Auslösers und Angriffsinformationen.

4. Bereinigung

   In diesem Abschnitt finden Sie reduzierbare Abschnitte mit Aktionen, die von GravityZone automatisch durchgeführt wurden, und empfohlene Schritte, die Sie befolgen können, um den Vorfall zu bereinigen.

5. Zwischenablage für Notizen

   Klicken Sie auf die Schaltfläche **Notizen**, um eine Zwischenablage zu öffnen, in der Sie Notizen zum aktuellen Vorfall hinzufügen können. Sie können diese Notizen einsehen, wenn Sie den Vorfall zu einem späteren Zeitpunkt erneut aufrufen.

6. Vorfallstatusleiste

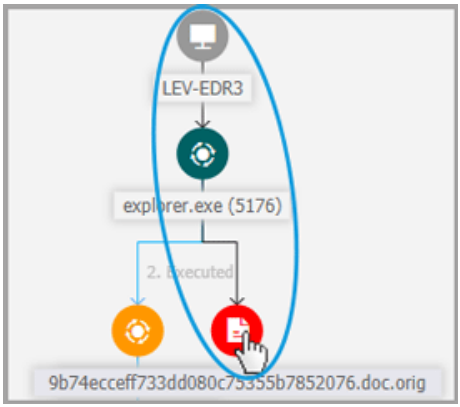
   Die Statusleiste zeigt Details zur ID des Vorfalls, zu Uhrzeit und Datum der Erstellung, zum Status, zum Auslöser des Vorfalls und zum Endpunkt, den er beeinträchtigt. Mit einem Klick auf die Schaltfläche **Zurück** gelangen Sie zurück zur Hauptseite **Vorfälle**.

Sicherheitsereignisknoten

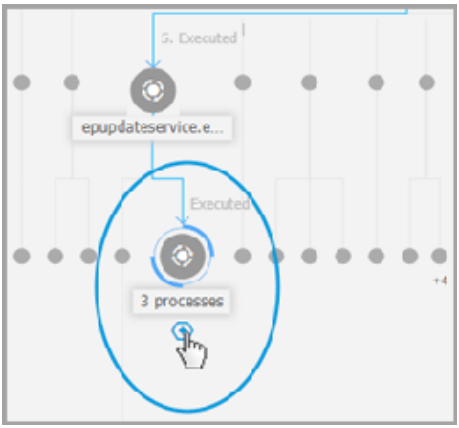
Wissenswertes zu den Sicherheitsereignisknoten:

- Jeder Knoten steht für ein bestimmtes Element, das an dem untersuchten Vorfall beteiligt ist.

- Alle Knoten, aus denen sich der kritische Pfad zusammensetzt, werden standardmäßig im Detail angezeigt, wenn Sie das Ereignis öffnen. Alle anderen Elemente werden der Übersichtlichkeit halber ausgeblendet.
  - Wenn Sie den Mauszeiger über einen Knoten bewegen, der nicht Bestandteil des kritischen Pfades ist, wird dieser hervorgehoben und der Pfad zum Ursprungspunkt angezeigt, ohne dass der kritische Pfad unterbrochen wird.



- Drei oder mehr Ereignisknoten vom gleichen Aktionstyp, die von einem übergeordneten Knoten ausgehen, werden zu einem erweiterbaren Clusterknoten zusammengefasst.



  - Nur Knoten ohne untergeordnete Elemente werden beim Reduzieren des Clusterknotens aus dem Ereignisdiagramm ausgeblendet.
  - Knoten, bei denen verdächtige Aktivitäten erkannt wurden, werden dem Clusterknoten nicht hinzugefügt.
- Mit einem Klick auf einen Knoten können Sie die folgenden Details anzeigen:
  - Der Pfad zum Endpunktknoten und alle beteiligten Elemente werden in Blau hervorgehoben.
  - Eine Seitenleiste mit erweiterbaren Abschnitten, die Details zu ausgewählten Knoten, Warnmeldungen zu Funden, verfügbare Aktionen und Empfehlungen anzeigen. Unter „Knotendetails“ (S. 325) finden Sie weitere Informationen.
- Die Knoten sind durch Pfeillinien verbunden, die den Verlauf der Aktionen anzeigen, die während des Vorfalls auf dem Endpunkt stattgefunden haben. Jede Linie ist mit dem Aktionsnamen und einer chronologischen Nummerierung versehen.

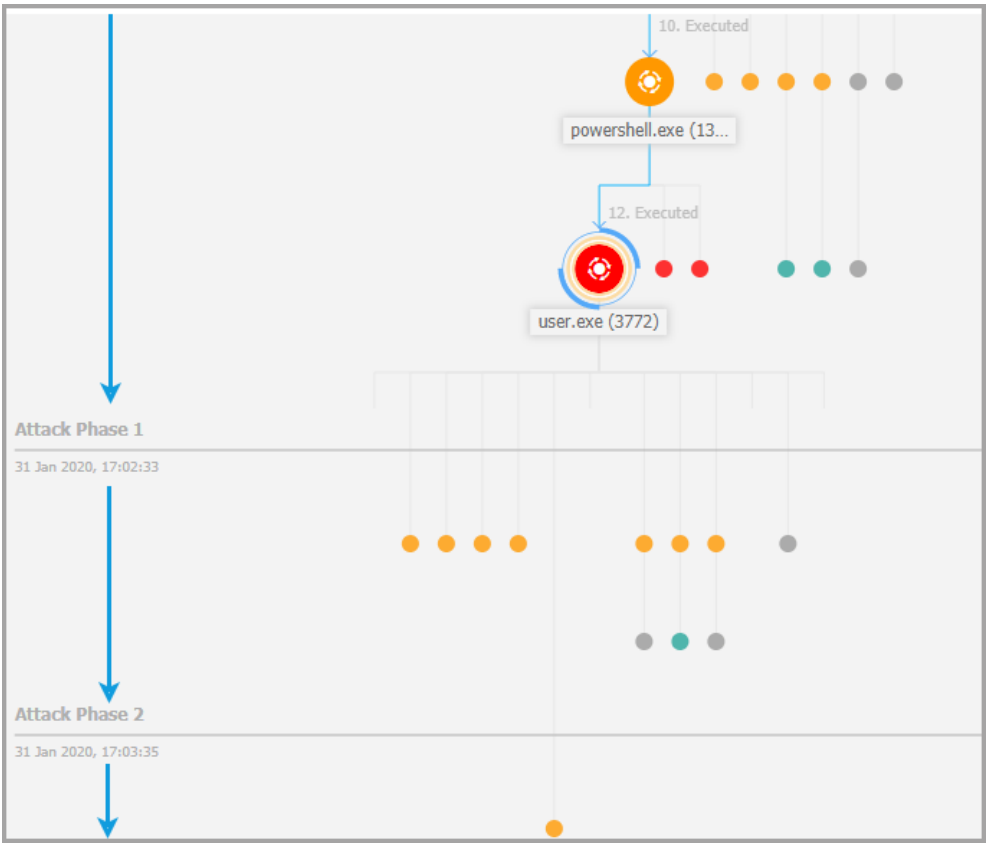
Die folgenden Elemente eines Vorfalls können als Knoten dargestellt werden:

Knotentyp	Beschreibung
Endpunkt	Zeigt Details zum Endpunkt und den Status des Patch-Managements an.
Domain	Zeigt Informationen zum Domain-Host und seinen Endpunkten an.

Knotentyp	Beschreibung
Prozess	Zeigt Details über die Rolle des Prozesses im jeweiligen Vorfall, Dateiinformationen, Details zu Prozessausführungen, Netzwerkpräsenz und weitere Untersuchungsoptionen an.
Datei	Zeigt Details über die Rolle der Datei im jeweiligen Vorfall sowie Dateiinformationen, Netzwerkpräsenz und weitere Untersuchungsoptionen an.
Registrierung	Zeigt Registrierungsinformationen und Details zum übergeordneten Prozess an.

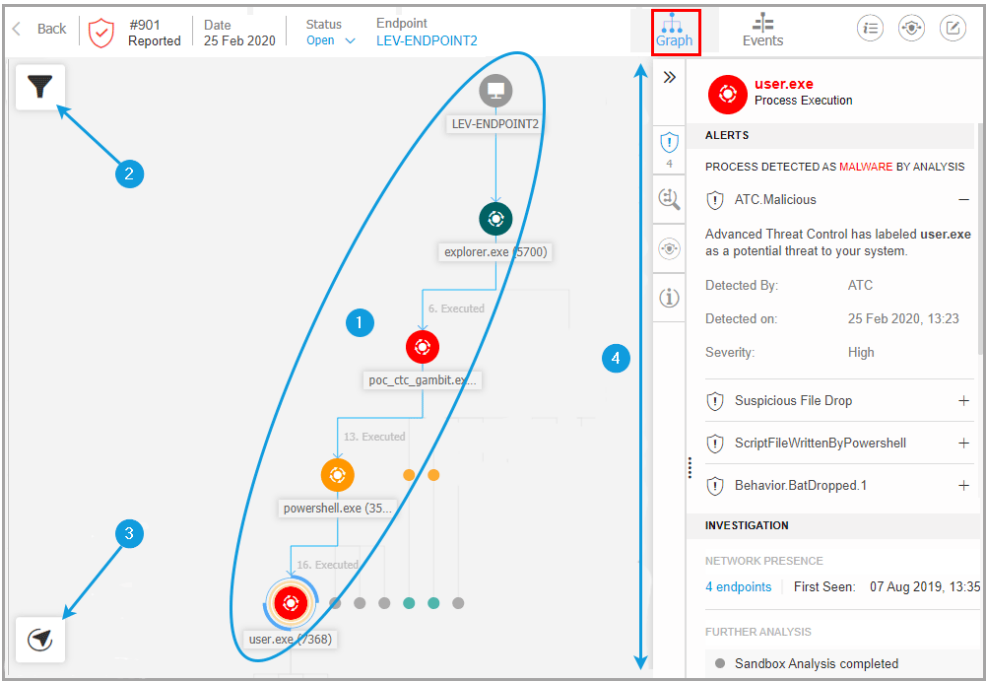
Diagramm

Das **Diagramm** ist eine interaktive grafische Darstellung des untersuchten Vorfalls und seines Kontextes. Hier ist die Abfolge der Elemente hervorgehoben, die direkt an der Auslösung beteiligt waren. Dies ist der so genannte **kritische Pfad** des Vorfalls. Sämtliche anderen beteiligten Elemente werden standardmäßig minimiert angezeigt. Bei komplexen Vorfällen, die sich mit der Zeit verändern, zeigt das Diagramm jede einzelne Phase des Angriffs an.



Mehrstufiger Angriff

Mit den Filteroptionen des Diagramms kann das Vorfallsdiagramm für mehr Übersichtlichkeit benutzerdefiniert angepasst werden. Hinzu kommen Funktionen zur Navigation durch das Vorfallsdiagramm und Detailfenster mit weiteren Informationen zu jedem Element.



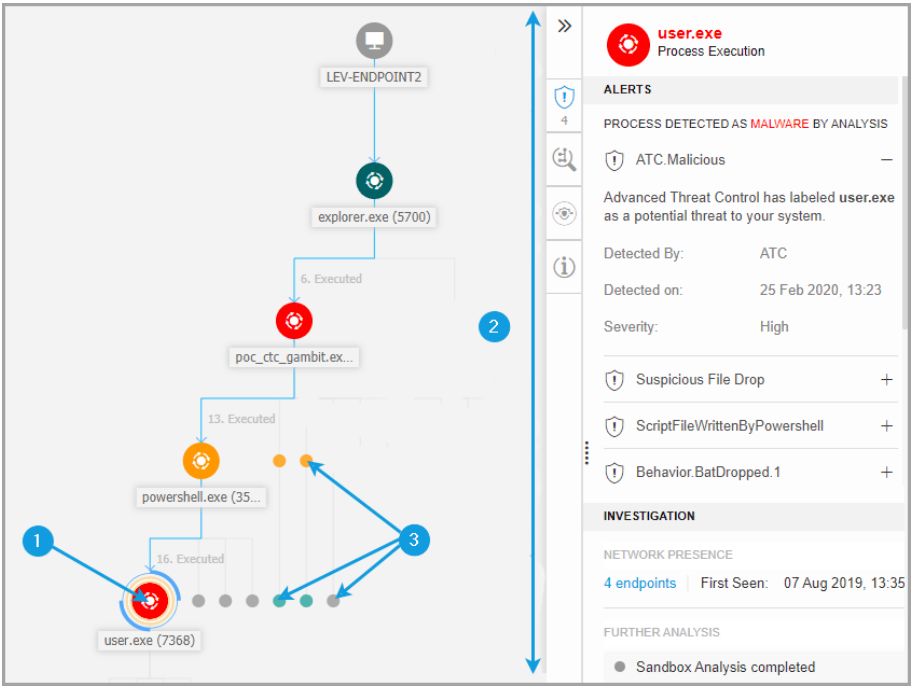
Diagrammreiter

1. Kritischer Pfad
2. Filtermenü
3. Navigationsmenü
4. Bereich Knotendetails

Kritischer Pfad

Der **kritische Pfad** ist die Abfolge der verbundenen Sicherheitsereignisse, die zur Auslösung einer Warnmeldung geführt haben, beginnend mit dem Einstiegspunkt im Netzwerk bis hin zum Ereignisknoten, der den Vorfall ausgelöst hat. Der kritische Pfad des Vorfalls, samt aller dazugehörigen Ereignisknoten, wird im Diagramm standardmäßig hervorgehoben dargestellt; alle anderen Elemente sind minimiert dargestellt.

Der Auslöserknoten hebt sich durch eine weitere Markierung (zwei orangefarbene Kreise rechts und links neben dem Knoten) deutlich von den anderen Elementen im Diagramm ab. Neben dem Vorfallsdiagramm wird standardmäßig ein entsprechendes Infofeld mit weiteren Einzelheiten zum Auslöserknoten angezeigt.



Kritischer Pfad

1. Auslöserknoten
2. Knotendetailansicht mit kategorisierten Informationen und expandierbaren Bereichen
3. Minimiert dargestellte Knoten, die indirekt am Vorfall beteiligt sind

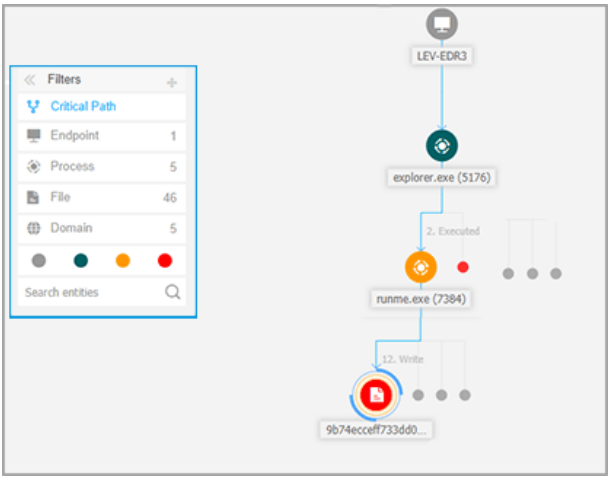
Beachten Sie

Wenn Sie auf ein anderes Element als den Auslöserknoten klicken, wird der kritische Pfad unterbrochen und der Pfad zum Ursprung vom ausgewählten Knoten vorwärts bis zum Endpunktknoten hervorgehoben.

Filter

Im **Filter**-Menü finden Sie erweiterte Filteroptionen, über die Sie das Vorfallsdiagramm anpassen können, indem Sie seine Elemente entweder nach Art oder Relevanz hervorheben oder für mehr Übersichtlichkeit und eine schnellere Analyse ausblenden.

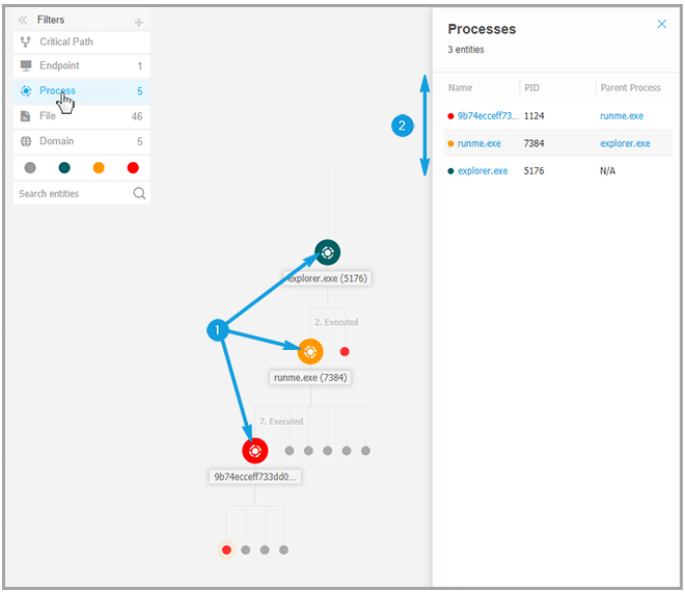
Sie können auf das ✣ **Ziehen**-Symbol klicken und mit festgehaltener Maustaste das schwebende Filterfenster an einer beliebigen Stelle im Vorfallsdiagramm positionieren.



Filtermöglichkeiten im Vorfallsdiagramm

Bei Auswahl eines Filters nach Elementart:

1. Das Vorfallsdiagramm zoomt aus der Ansicht heraus und hebt alle Elemente des ausgewählten Typs hervor und blendet andere Elemente aus.
2. Es wird ein neuer Bereich mit einer Liste aller hervorgehobenen Elemente angezeigt.



Beachten Sie
Durch Auswahl eines Elements aus der Liste wird dieses Element im Vorfallsdiagramm hervorgehoben und ein Detailbereich mit Informationen zu diesem Element angezeigt. Es kann jeweils nur ein Filter angewendet werden.

Die Filteroptionen umfassen:

- **Kritischer Pfad**: Hebt den kritischen Pfad des Vorfalls hervor.
- **Endpunkt**: Hebt alle von dem Vorfall betroffenen Endpunkte hervor.
- **Prozess**: Hebt alle Knoten vom Typ Prozess hervor, die an dem Vorfall beteiligt sind.
- **Datei**: Hebt alle Knoten vom Typ Datei hervor, die an dem Vorfall beteiligt sind.

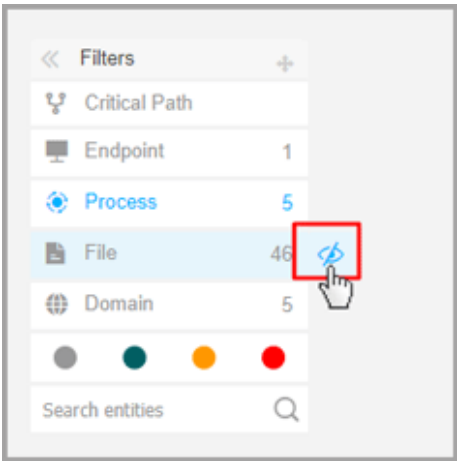
- **Domain**: Hebt alle Knoten vom Typ Domain hervor, die an dem Vorfall beteiligt sind.
- **Registrierung**: Hebt alle Knoten vom Typ Registrierung hervor, die an dem Vorfall beteiligt sind.
- **Elementrelevanz**: Sie können Elemente auch nach ihrer Relevanz für den Vorfall filtern.
  - **Neutraler Knoten**: Elemente ohne direkte Auswirkung auf den Sicherheitsvorfall.
  - **Wichtiger Knoten**: Elemente mit relevanter Beteiligung am Sicherheitsvorfall.
  - **Ursprungsknoten**: Einfallstor des Angriffs im Netzwerk.
  - **Verdächtiger Knoten**: Elemente, die sich verdächtig verhalten und direkt an dem Sicherheitsvorfall beteiligt sind.
  - **Schädlicher Knoten**: Elemente, die Netzwerkschäden verursacht haben.

    Beachten Sie
    Wenn Sie den Mauszeiger über einen der Farbfilter bewegen, wird angezeigt, wie viele Elemente mit gleicher Relevanz an dem Vorfall beteiligt sind.

- **Entitäten suchen**: Über dieses Suchfeld können Sie nach den Namen oder Dateiendungen von Vorfallselementen suchen. Die Ergebnisse der Suche werden im Seitenbereich angezeigt.

Wenn keine Filter ausgewählt sind, wird das Vorfallsdiagramm in den Standardzustand zurückgesetzt, wobei Endpunkt-, Ursprungs- und Auslöserelemente hervorgehoben und die anderen Elemente ausgeblendet werden.

Sie können auch bestimmte Elemente aus dem Vorfallsdiagramm ausblenden, indem Sie auf die Schaltfläche **Einblenden/Ausblenden** klicken, die angezeigt wird, wenn Sie den Mauszeiger über folgende Filter bewegen: Datei, Domain und Registrierung.



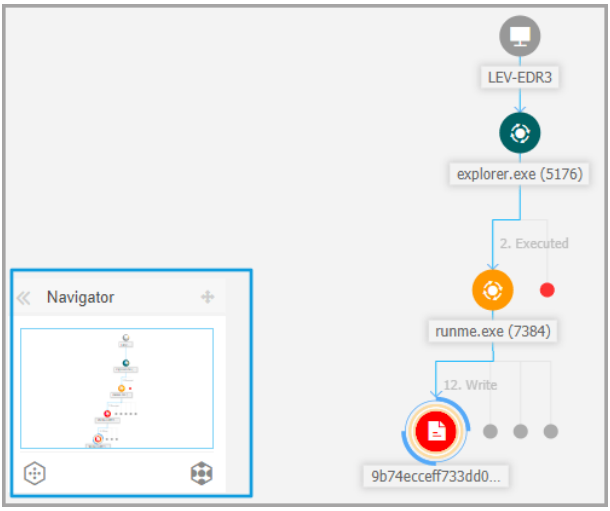
Wird ein Elementtyp ausgeblendet wird die Darstellung des Vorfallsdiagramms aktualisiert. Dabei werden alle entsprechenden Elemente entfernt, auch wenn sie verkleinert dargestellt sind, mit Ausnahme des Auslöserknotens und der Knoten mit untergeordneten Elementen.

Navigation

Über die **Navigation** können Sie sich schnell durch das Vorfallsdiagramm bewegen und alle angezeigten Elemente mit Hilfe der Mini-Karte und der verschiedenen Visualisierungsebenen erkunden.

Sie können auf das ✣ **Ziehen**-Symbol klicken und mit festgehaltener Maustaste das schwebende Filterfenster an einer beliebigen Stelle im Vorfallsdiagramm positionieren.

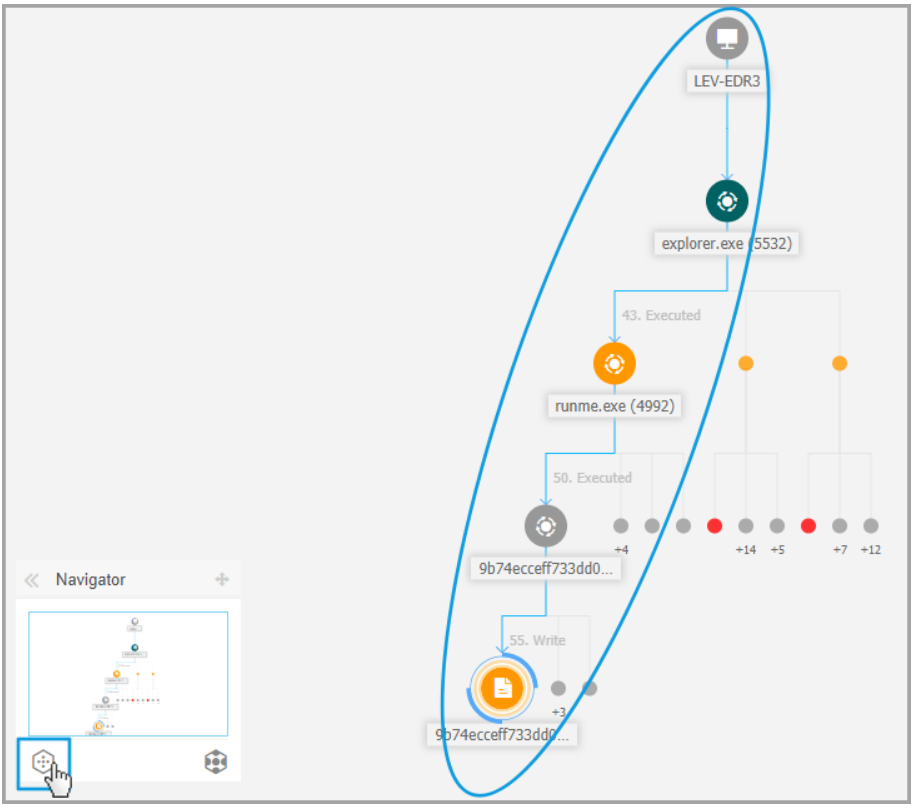
Die **Navigation** wird standardmäßig ausgeblendet. Wird sie erweitert, zeigt das Menü die miniaturisierte Version des gesamten Vorfallsdiagramms und Schaltflächen zur Einstellung der Darstellungsebene an.



Navigation

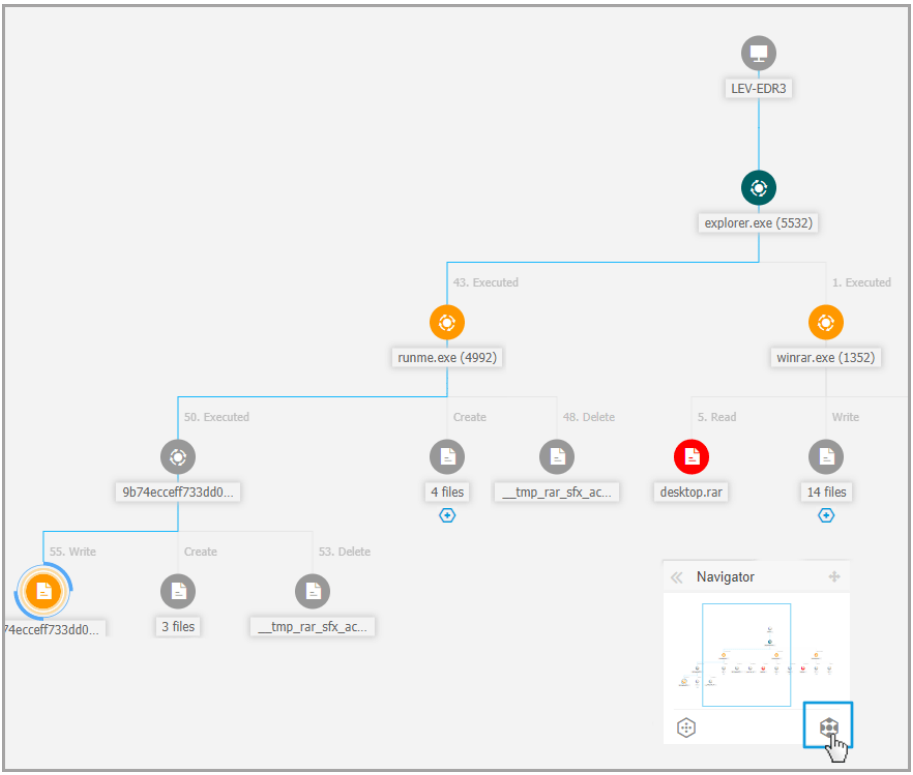
Im **Navigationsmenü** finden Sie zwei Schaltflächen, mit denen Sie festlegen können, wie Sie das Vorfallsdiagramm anzeigen möchten: die Schaltfläche **Weniger Details** und die Schaltfläche **Mehr Details**.

Mit einem Klick auf die Schaltfläche **Weniger Details** wird das Diagramm in den Standardzustand zurückgesetzt und nur der kritischen Pfad des Vorfalls hervorgehoben.



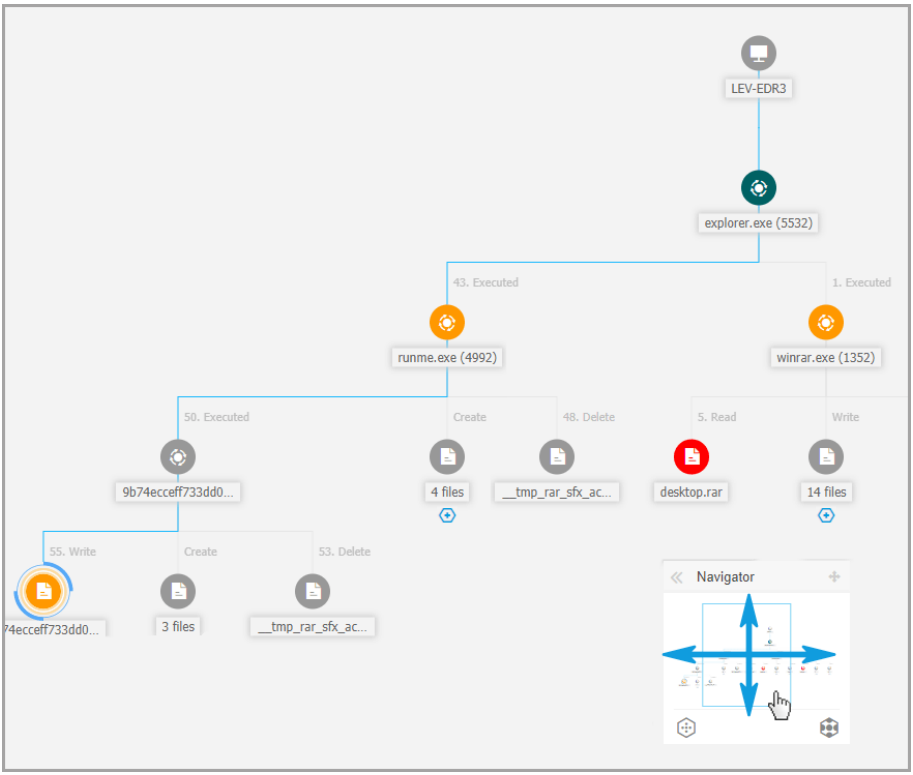
Übersichtsdarstellung

Mit einem Klick auf die Schaltfläche **Mehr Details** werden alle Elemente im Vorfallsdiagramm erweitert und alle Knoten und Knotencluster hervorgehoben.



Vergrößerte Darstellung

Wenn der Vorfall vergrößert dargestellt wird und alle Elemente hervorgehoben sind, kann sich das Diagramm über die Bildschirmgrenzen hinaus erstrecken. Halten Sie in diesem Fall die Kartenauswahl in der Mini-Karte der Navigation gedrückt und ziehen Sie sie, um schnell zum gewünschten Bereich des Vorfallsdiagramms zu navigieren, oder ziehen Sie den Diagrammbereich einfach in die gewünschte Richtung.

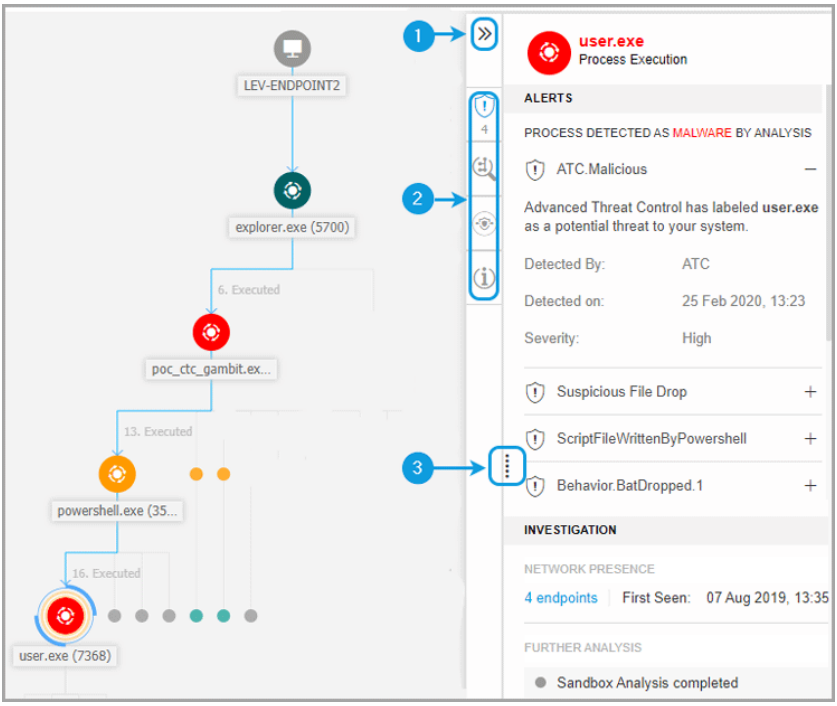


Mini-Karte-Auswahl

Knotendetails

Der Bereich **Knotendetails** enthält Abschnitte mit detaillierten Informationen zum ausgewählten Knoten, einschließlich Präventiv- oder Bereinigungsmaßnahmen, die Sie ergreifen können, um den Vorfall zu beheben, Details über die Art der Fundes und die auf dem Knoten gefundenen Warnmeldungen, Netzwerkpräsenz, Details zur Prozessausführung, zusätzliche Empfehlungen zum Umgang mit dem Sicherheitsereignis bzw. Aktionen zur weiteren Untersuchung des Elements.

Wenn Sie diese Informationen anzeigen und Aktionen in der Tafel durchführen möchten, wählen Sie einen Knoten im Sicherheitsereignis-Diagramm.



Bereich Knotendetails

1. Sie können den Bereich **Knoten-Details** ausblenden, indem Sie auf die Schaltfläche **Reduzieren** klicken.
2. Die Informationen im Bereich **Knotendetails** sind in vier Kategorien eingeteilt:
   - **WARNMELDUNGEN**

     In diesem Bereich werden die Funde aufgeführt, die auf dem ausgewählten Knoten ausgelöst wurden, einschließlich Details zur Bitdefender-Technologie, mit der das Element gefunden wurde, die Ursache für die Erkennung, den Namen des Fundes sowie das Datum der Erkennung.
   - **UNTERSUCHUNG**

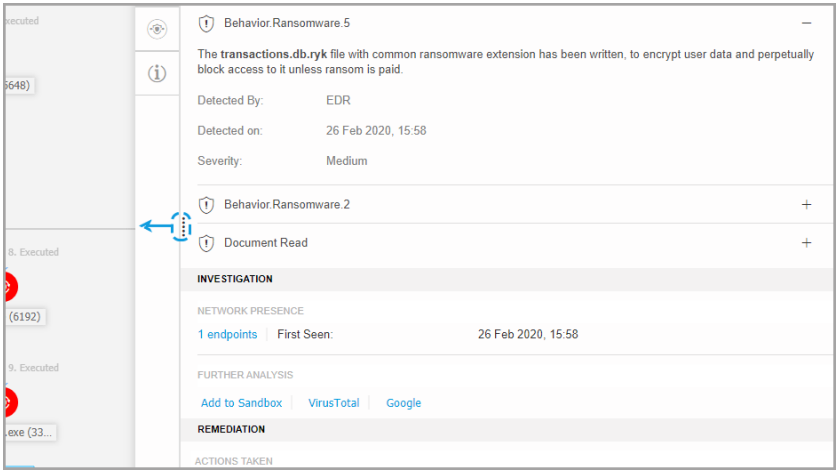
     In diesem Bereich werden die Zeitstempel des ursprünglichen Fundes sowie sämtliche Endpunkte aufgeführt, auf denen dieses Element gefunden wurde.
   - **BEREINIGUNG**

In diesem Bereich werden Aktionen angezeigt, die von GravityZone automatisch durchgeführt wurden, sowie Aktionen gegen die Bedrohung, die Sie sofort durchführen können. Hierbei helfen die ebenfalls angezeigten detaillierten Empfehlungen für jeden Fund, mit denen die Sicherheit Ihrer Umgebung noch weiter erhöht werden kann.

- **INFO**

  In diesem Bereich werden allgemeine Informationen zu jeder Datei angezeigt sowie spezifische Informationen je nach Typ des Knotens.

3. Sie können den Bereich **Knotendetails** vergrößern, indem Sie mit der Maus den Rand des Bereichs zur Mitte des Fensters ziehen.



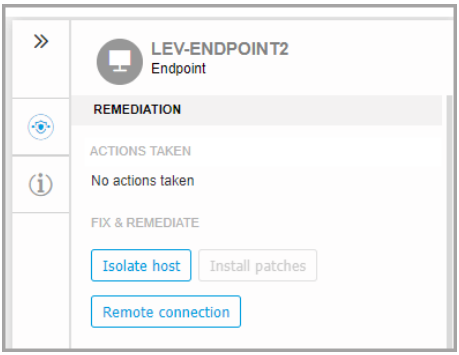
Vergrößerter Bereich Knotendetails

Detailbereich für Endpunkt-Knoten

Der Bereich **Knotendetails** für Endpunkte enthält zwei Kategorien:

- **BEREINIGUNG**

  Hier werden Informationen zu Aktionen angezeigt, die GravityZone automatisch gegen die Bedrohung durchgeführt hat, und solche, die Sie selbst durchführen können:

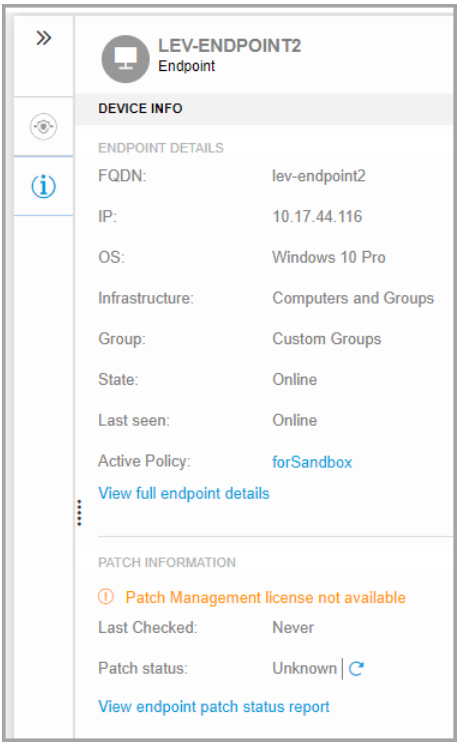


- **Host isolieren** - Mit dieser Aktion isolieren Sie den Endpunkt vom Netzwerk.
- **Installieren von Patches** - Mit dieser Aktion können Sie einen fehlenden Sicherheits-Patch auf dem entsprechenden Endpunkt installieren. Diese Option wird nur angezeigt, wenn das Modul Patch-Verwaltung aktiv ist, das über eine separate Lizenz erworben werden kann. Weitere Informationen finden Sie unter Patch-Installation.
- **Remote-Verbindung** - Mit dieser Aktion können Sie eine Remote-Verbindung zu dem am aktuellen Vorfall beteiligten Endpunkt herzustellen und eine Reihe von benutzerdefinierten Shell-Befehlen direkt auf dem Betriebssystem auszuführen, um die Bedrohung sofort zu beheben oder Daten für die weitere Untersuchung zu sammeln.

  Durch Anklicken dieser Schaltfläche wird das Fenster Remote-Verbindung angezeigt.

- **GERÄTE-INFO**

  Hier werden allgemeine Informationen zum betroffenen Endpunkt angezeigt, z. B. Name des Endpunkts, Betriebssystem, relevante Gruppe, Status, aktive Richtlinien und einen Link, über den ein Fenster mit den vollständigen Informationen zum Endpunkt geöffnet werden kann.



Hier werden auch die Anzahl der installierten Patches, die fehlgeschlagenen Patch-Installationen, fehlende Patches (egal ob sicherheitsrelevant oder nicht) und andere Informationen angezeigt. Hier können Sie auch einen Endpunkt-Patch-Statusbericht erzeugen. Dieser Abschnitt wird bei Bedarf für den Zielendpunkt angezeigt.

Auf dieser Tafel können die folgenden Aktionen durchgeführt werden:

– Patch-Informationen zum Endpunkt anzeigen. Klicken Sie in diesem Abschnitt auf **Neu laden**, um Patch-Details anzuzeigen.

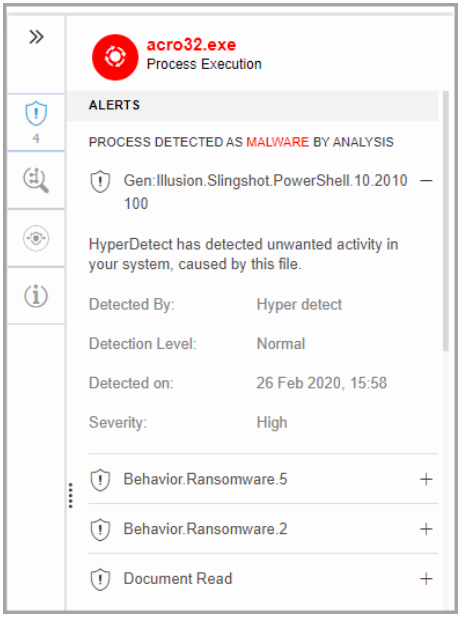
– Den Patch-Statusbericht für den Endpunkt anzeigen. Um den Bericht zu erzeugen, klicken Sie auf **Endpunkt-Patch-Statusbericht anzeigen**.

Detailbereich für Prozess-Knoten

Der Bereich **Knotendetails** für Prozess-Knoten enthält vier Kategorien:

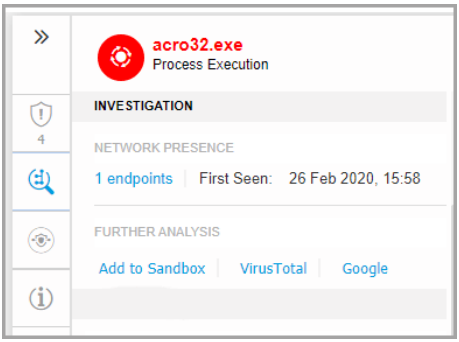
- **WARNMELDUNGEN**

  In diesem Bereich werden die Funde aufgeführt, die auf dem ausgewählten Knoten ausgelöst wurden, einschließlich Details zur Bitdefender-Technologie, mit der die Entität gefunden wurde, die Ursache für die Erkennung, den Namen des Fundes sowie das Datum der Erkennung. Die Beschreibung der Warnmmeldungen entspricht den neuesten MITRE-Standards.

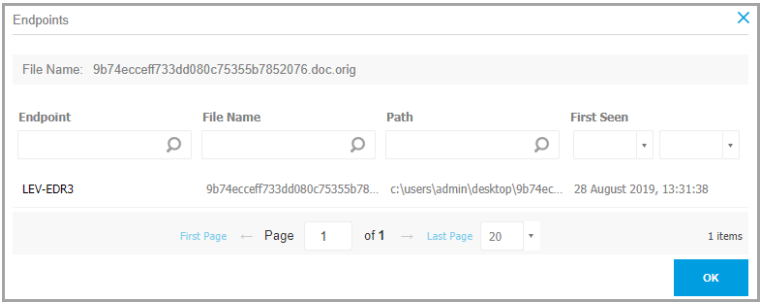


- **UNTERSUCHUNG**

  In diesem Bereich werden die Zeitstempel des ursprünglichen Fundes sowie sämtliche Endpunkte aufgeführt, auf denen dieses Element gefunden wurde.



Diese Liste wird angezeigt, wenn Sie auf die Zahl klicken, die im Feld **Endpunkte** angezeigt wird. Daraufhin wird ein neues Fenster angezeigt.

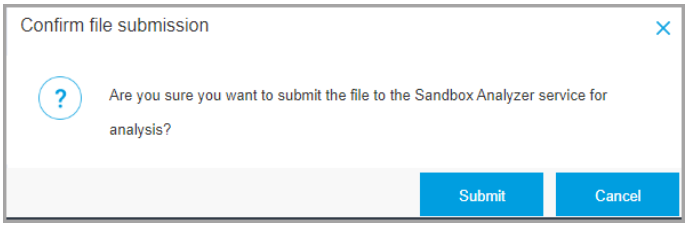


Hier stehen auch Möglichkeiten zur Analyse durch interne Komponenten und externe Lösungen zur Verfügung.

Folgende Aktionen stehen zur Verfügung:

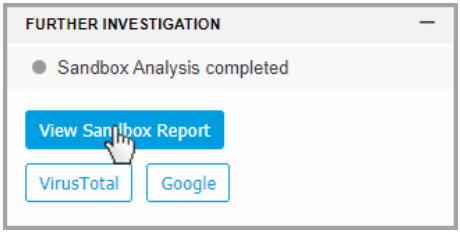
– **Zur Sandbox hinzufügen** - Verwenden Sie diese Aktion, um einen Sandbox Analyzer-Bericht zu erstellen.

  Nach einem Klick auf **Zur Sandbox hinzufügen** werden Sie in einem neuen Fenster aufgefordert, die Dateiübermittlung zu bestätigen.



Nach der Bestätigung werden Sie automatisch zur Übermittlungsseite weitergeleitet.

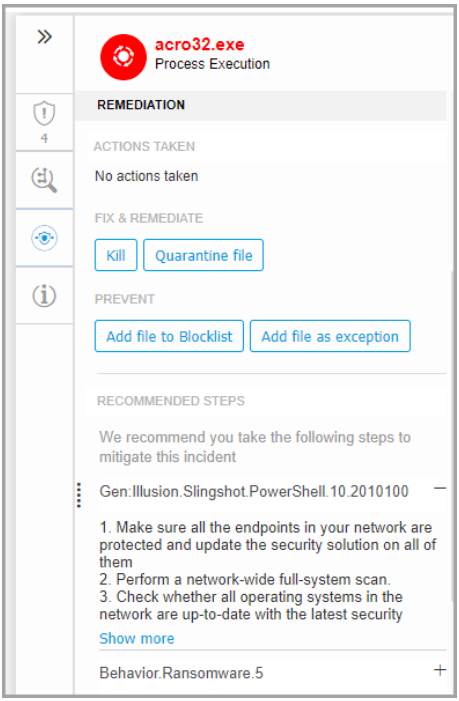
Klicken Sie nach Abschluss der Analyse auf **Sandbox-Bericht anzeigen**, um den vollständigen Bericht zu öffnen.



- **VirusTotal** - Mit dieser Aktion können Dateien zur Analyse an VirusTotal übermittelt werden.
- **Google** - Mit dieser Aktion können Sie nach dem Hash-Wert einer Datei suchen.

- **BEREINIGUNG**

  Hier werden Informationen zu Aktionen angezeigt, die GravityZone automatisch gegen die Bedrohung durchgeführt hat, und solche, die Sie selbst durchführen können:



- **Beenden** - Mit dieser Aktion können Sie die Ausführung eines Prozesses abbrechen. Durch diese Aktion wird eine Prozessbeendigungsaufgabe erstellt, die dann in der Prozessausführungsleiste angezeigt wird. `System32`- und Bitdefender-Prozesse können mit dieser Aktion nicht beendet werden.
- **Datei in Quarantäne verschieben** - Mit dieser Aktion wird das Objekt in die Quarantäne verschoben und an der Ausführung gehindert. Für diese Aktion muss das Firewall-Modul auf dem Zielendpunkt installiert sein.
- **Datei zur Blockierliste hinzufügen** - Verwalten Sie blockierte Elemente im Abschnitt Blockierliste.
- **Datei als Ausnahme hinzufügen** - Mit dieser Option können Sie unbedenkliche Aktivitäten unter einer bestimmten Richtlinie ausschließen. Wenn Sie diese Aktion wählen, wird ein Konfigurationsfenster geöffnet, in dem Sie die Richtlinie auswählen müssen, zu der Sie die Ausnahme definieren möchten.

Die Ausschlüsse können Sie unter **Richtlinien > Malware-Schutz > Einstellungen** verwalten.

– **Als EDR-Ausschluss hinzufügen** - Verwenden Sie diese Option, um eine benutzerdefinierte Regel zu erstellen, die den Prozess nicht mehr als verdächtige oder schädliche EDR-Erkennung behandelt.

1. Wenn Sie auf die Schaltfläche **Als EDR-Ausschluss hinzufügen** klicken, wird ein neues Fenster mit der Aufforderung angezeigt, die Aktion zu bestätigen oder abzubrechen.
2. Nachdem Sie die Aktion bestätigt haben, werden Sie von GravityZone benachrichtigt, dass die neue Regel im Raster Ausschlussregeln verfügbar ist. Beachten Sie, dass die Namen aller Regeln, die aus dem Vorfalldiagramm heraus erstellt werden, mit der Vorfallnummer beginnen.

Beachten Sie
Wenn Sie die Regeldetails zur Bearbeitung öffnen, werden Sie feststellen, dass alle Kriterien für diese Regel automatisch ausgefüllt wurden und ein schreibgeschütztes Kriterium mit dem Namen der Warnmeldung hinzugefügt wurde.

Wichtig
Die Funktion **Als EDR-Ausschluss hinzufügen** ist ausschließlich verfügbar für:

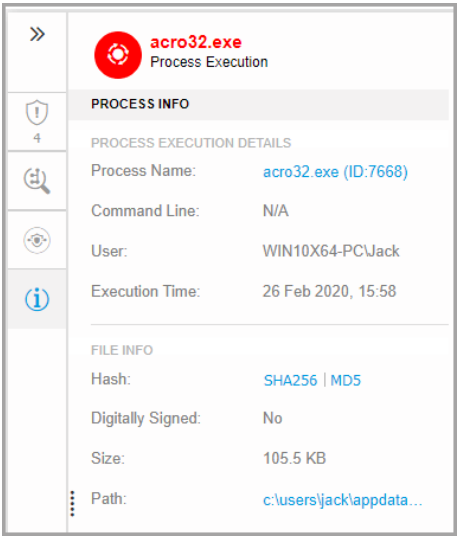
- durch die EDR-Technologie ausgelöste Warnmeldungen
- von einem anderen Prozess erzeugte Knoten
- verdächtige und schädliche Knoten

Wenn der ausgeschlossene Prozess Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, nicht mehr im Vorfallraster generiert. Die bestehenden Ereignisse stehen weiterhin zur Ansicht und Analyse auf der Seite Suche zur Verfügung.
Wenn der ausgeschlossene Prozess nicht Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, weiterhin im Vorfallraster generiert, aber dieser Prozess nicht mehr als verdächtig oder schädlich eingestuft.

Dieser Abschnitt enthält auch detaillierte Empfehlungen für jede Warnmeldung, die auf dem ausgewählten Knoten gefunden wird, um Sie bei der Eindämmung des Vorfalls zu unterstützen und das Sicherheitsniveau Ihrer Umgebung zu erhöhen.

- **PROZESS-INFO**

  Hier werden Details zum jeweiligen Prozess-Knoten angezeigt, z. B. Name des Prozesses, ausgeführte Befehlszeile, Benutzer, Zeitpunkt der Ausführung, Dateiursprung und Pfad, Hash-Wert und digitale Signatur.



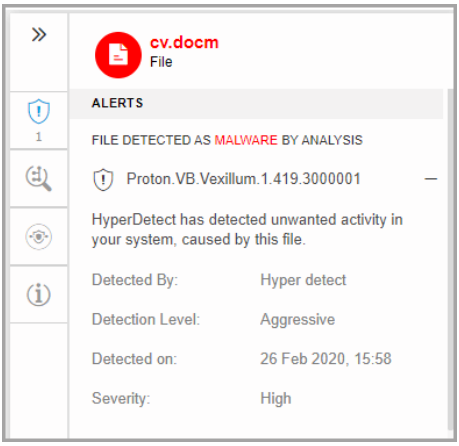
  Wenn Sie den Hash-Wert kopieren möchten, um in an anderer Stelle einfügen zu können, klicken Sie im Feld **Hash** auf die entsprechenden Hash-Algorithmen und anschließend auf **In Zwischenablage kopieren**. Dann können Sie den Hash-Wert einer Datei z. B. in die **Blockierliste** aufnehmen. Näheres hierzu unter **Dateien zur Blockierliste hinzufügen**.

Detailbereich für Datei-Knoten

Der Bereich **Knotendetails** für Datei-Knoten enthält vier Kategorien:

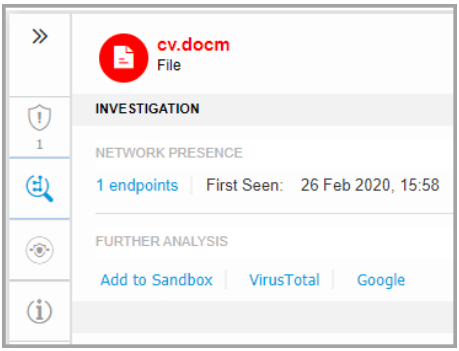
- **WARNMELDUNGEN**

  In diesem Bereich werden die Funde aufgeführt, die auf dem ausgewählten Knoten ausgelöst wurden, einschließlich Details zur Bitdefender-Technologie, mit der die Entität gefunden wurde, die Ursache für die Erkennung, den Namen des Fundes sowie das Datum der Erkennung. Die Beschreibung der Warnmmeldungen entspricht den neuesten MITRE-Standards.

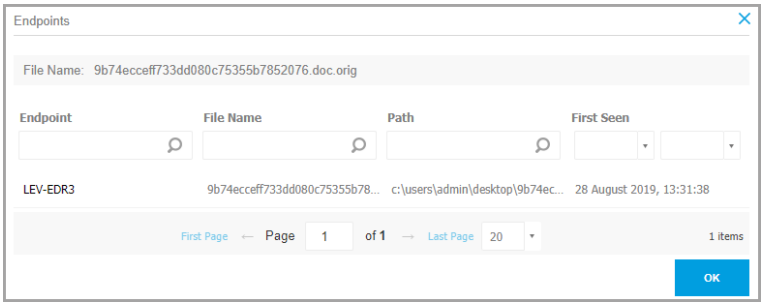


- **UNTERSUCHUNG**

  In diesem Bereich werden die Zeitstempel des ursprünglichen Fundes sowie sämtliche Endpunkte aufgeführt, auf denen dieses Element gefunden wurde.



  Diese Liste wird angezeigt, wenn Sie auf die Zahl klicken, die im Feld **Endpunkte** angezeigt wird. Daraufhin wird ein neues Fenster angezeigt.

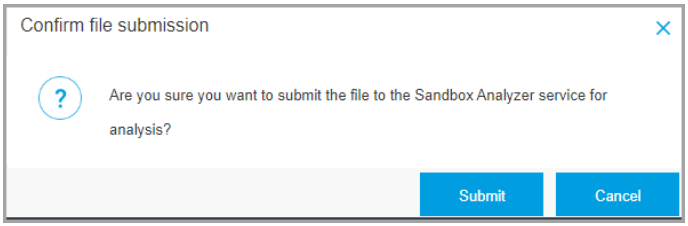


Hier stehen auch Möglichkeiten zur Analyse durch interne Komponenten und externe Lösungen zur Verfügung.

Folgende Aktionen stehen zur Verfügung:

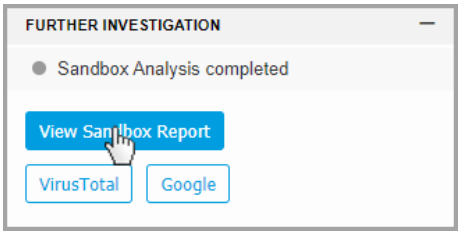
– **Zur Sandbox hinzufügen** - Verwenden Sie diese Aktion, um einen Sandbox Analyzer-Bericht zu erstellen.

  Nach einem Klick auf **Zur Sandbox hinzufügen** werden Sie in einem neuen Fenster aufgefordert, die Dateiübermittlung zu bestätigen.



  Nach der Bestätigung werden Sie automatisch zur Übermittlungsseite weitergeleitet.

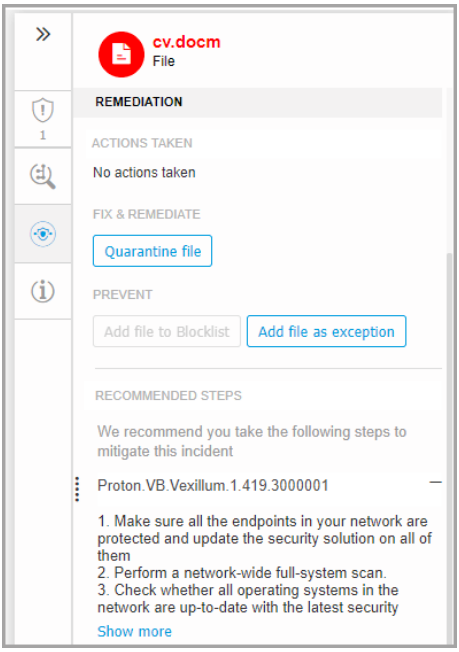
  Klicken Sie nach Abschluss der Analyse auf **Sandbox-Bericht anzeigen**, um den vollständigen Bericht zu öffnen.



- **VirusTotal** - Mit dieser Aktion können Dateien zur Analyse an VirusTotal übermittelt werden.
- **Google** - Mit dieser Aktion können Sie nach dem Hash-Wert einer Datei suchen.

- **BEREINIGUNG**

  Hier werden Informationen zu Aktionen angezeigt, die GravityZone automatisch gegen die Bedrohung durchgeführt hat, und solche, die Sie selbst durchführen können:



- **Datei in Quarantäne verschieben** - Mit dieser Aktion wird das Objekt in die Quarantäne verschoben und an der Ausführung gehindert. Für diese Aktion muss das Firewall-Modul auf dem Zielendpunkt installiert sein.
- **Datei zur Blockierliste hinzufügen** - Verwalten Sie blockierte Elemente im Abschnitt Blockierliste.
- **Datei als Ausnahme hinzufügen** - Mit dieser Option können Sie unbedenkliche Aktivitäten unter einer bestimmten Richtlinie ausschließen. Wenn Sie diese Aktion wählen, wird ein Konfigurationsfenster geöffnet, in dem Sie die Richtlinie auswählen müssen, zu der Sie die Ausnahme definieren möchten. Die Ausschlüsse können Sie unter **Richtlinien > Malware-Schutz > Einstellungen** verwalten.
- **Als EDR-Ausschluss hinzufügen** - Verwenden Sie diese Option, um eine benutzerdefinierte Regel zu erstellen, die die Datei nicht mehr als verdächtige oder schädliche EDR-Erkennung behandelt.

1. Wenn Sie auf die Schaltfläche **Als EDR-Ausschluss hinzufügen** klicken, wird ein neues Fenster mit der Aufforderung angezeigt, die Aktion zu bestätigen oder abzubrechen.
2. Nachdem Sie die Aktion bestätigt haben, werden Sie von GravityZone benachrichtigt, dass die neue Regel im Raster Ausschlussregeln verfügbar ist. Beachten Sie, dass die Namen aller Regeln, die aus dem Vorfalldiagramm heraus erstellt werden, mit der Vorfallnummer beginnen.

Beachten Sie
Wenn Sie die Regeldetails zur Bearbeitung öffnen, werden Sie feststellen, dass alle Kriterien für diese Regel automatisch ausgefüllt wurden und ein schreibgeschütztes Kriterium mit dem Namen der Warnmeldung hinzugefügt wurde.

Wichtig
Die Funktion **Als EDR-Ausschluss hinzufügen** ist ausschließlich verfügbar für:

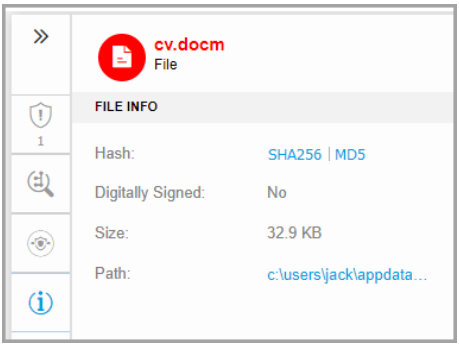
- durch die EDR-Technologie ausgelöste Warnmeldungen
- von einem anderen Prozess erzeugte Knoten
- verdächtige und schädliche Knoten

Wenn die ausgeschlossene Datei Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, nicht mehr im Vorfallraster generiert. Die bestehenden Ereignisse stehen weiterhin zur Ansicht und Analyse auf der Seite Suche zur Verfügung.
Wenn die ausgeschlossene Datei nicht Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, weiterhin im Vorfallraster generiert, aber dieser Prozess nicht mehr als verdächtig oder schädlich eingestuft.

Dieser Abschnitt enthält auch detaillierte Empfehlungen für jede Warnmeldung, die auf dem ausgewählten Knoten gefunden wird, um Sie bei der Eindämmung des Vorfalls zu unterstützen und das Sicherheitsniveau Ihrer Umgebung zu erhöhen.

- **DATEI-INFO**

  Hier werden Details zum jeweiligen Datei-Knoten angezeigt, z. B. Dateiursprung und Pfad, Hash-Wert und digitale Signatur.



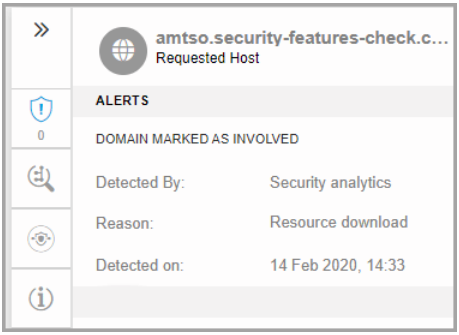
Wenn Sie den Hash-Wert kopieren möchten, um in an anderer Stelle einfügen zu können, klicken Sie im Feld **Hash** auf die entsprechenden Hash-Algorithmen und anschließend auf **In Zwischenablage kopieren**. Dann können Sie den Hash-Wert einer Datei z. B. in die **Blockierliste** aufnehmen. Näheres hierzu unter **Dateien zur Blockierliste hinzufügen**.

Detailbereich für Domain-Knoten

Der Bereich **Knotendetails** für Domain-Knoten enthält vier Kategorien:

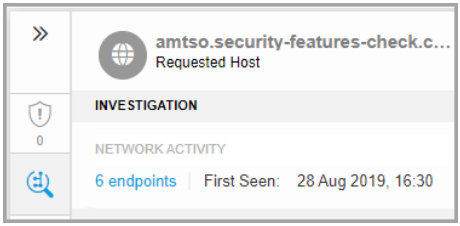
- **WARNMELDUNGEN**

  In diesem Bereich wird der Schweregrad des Fundes angezeigt, und zwar gemessen an der Bitdefender-Technologie, mit der die Entität gefunden wurde, die Ursache für die Erkennung sowie das Datum der Erkennung.

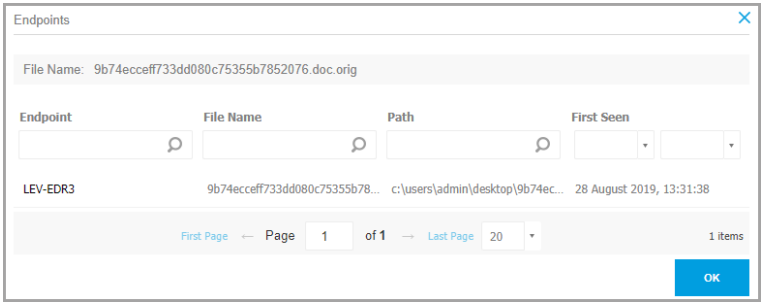


- **UNTERSUCHUNG**

  In diesem Bereich werden die Zeitstempel des ursprünglichen Fundes sowie sämtliche Endpunkte aufgeführt, auf denen dieses Element gefunden wurde.

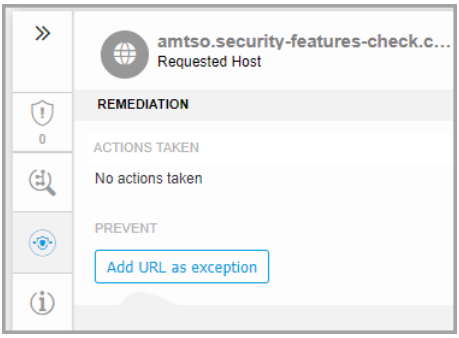


  Diese Liste wird angezeigt, wenn Sie auf die Zahl klicken, die im Feld **Endpunkte** angezeigt wird. Daraufhin wird ein neues Fenster angezeigt.



- **BEREINIGUNG**

  Hier werden Informationen zu Aktionen angezeigt, die GravityZone automatisch gegen die Bedrohung durchgeführt hat, und solche, die Sie selbst durchführen können:



- **URL als Ausnahme hinzufügen** - Mit dieser Option können Sie unbedenkliche Aktivitäten unter einer bestimmten Richtlinie ausschließen. Wenn Sie diese Aktion wählen, wird ein Konfigurationsfenster geöffnet, in dem Sie die Richtlinie auswählen müssen, zu der Sie die Ausnahme definieren möchten. Die Ausschlüsse können Sie unter **Richtlinien > Malware-Schutz > Einstellungen** verwalten.
- **Als EDR-Ausschluss hinzufügen** - Verwenden Sie diese Option, um eine benutzerdefinierte Regel zu erstellen, die die Domäne nicht mehr als verdächtige oder schädliche EDR-Erkennung behandelt.

  1. Wenn Sie auf die Schaltfläche **Als EDR-Ausschluss hinzufügen** klicken, wird ein neues Fenster mit der Aufforderung angezeigt, die Aktion zu bestätigen oder abzubrechen.
  2. Nachdem Sie die Aktion bestätigt haben, werden Sie von GravityZone benachrichtigt, dass die neue Regel im Raster Ausschlussregeln verfügbar ist. Beachten Sie, dass die Namen aller Regeln, die aus dem Vorfalldiagramm heraus erstellt werden, mit der Vorfallnummer beginnen.

Beachten Sie
Wenn Sie die Regeldetails zur Bearbeitung öffnen, werden Sie feststellen, dass alle Kriterien für diese Regel automatisch ausgefüllt wurden und ein schreibgeschütztes Kriterium mit dem Namen der Warnmeldung hinzugefügt wurde.

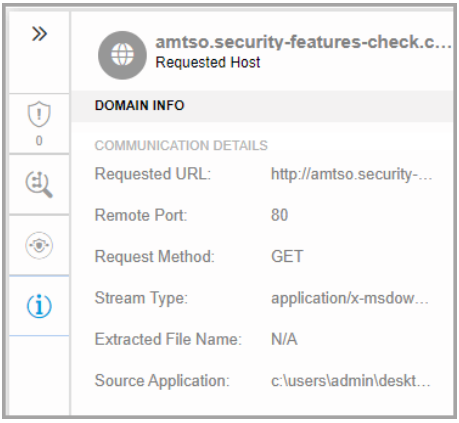
Wichtig
Die Funktion **Als EDR-Ausschluss hinzufügen** ist ausschließlich verfügbar für:

- durch die EDR-Technologie ausgelöste Warnmeldungen
- von einem anderen Prozess erzeugte Knoten
- verdächtige und schädliche Knoten

Wenn die ausgeschlossene Domäne Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, nicht mehr im Vorfallraster generiert. Die bestehenden Ereignisse stehen weiterhin zur Ansicht und Analyse auf der Seite Suche zur Verfügung.
Wenn die ausgeschlossene Domäne nicht Teil des kritischen Pfades des Vorfalls ist, werden zukünftige Vorfälle, die diesem Ausschlusskriterium entsprechen, weiterhin im Vorfallraster generiert, aber dieser Prozess nicht mehr als verdächtig oder schädlich eingestuft.

- **DOMAIN-INFO**

  Hier werden Details zur jeweiligen Domain angezeigt, z. B. angefragte URL, verwendeter Port, Anfragemethode, Streamtyp, Name der extrahierten Datei und Quellanwendung.



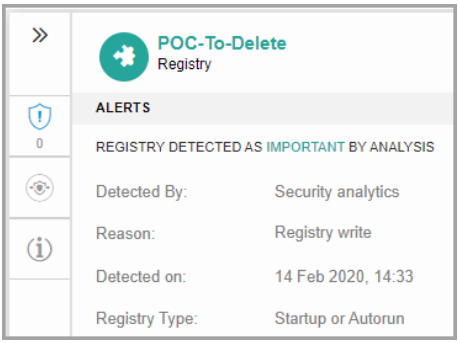
Detailbereich für Registrierungs-Knoten

Der Bereich **Knotendetails** für Registrierungs-Knoten enthält drei Kategorien:

- **WARNMELDUNGEN**

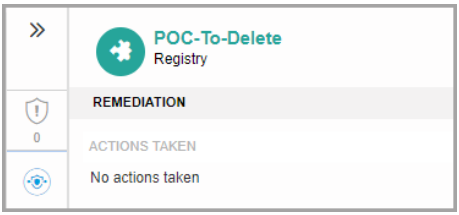
  In diesem Bereich wird der Schweregrad der Registrierungs-Manipulation angezeigt, und zwar gemessen an der Bitdefender-Technologie, mit der die

Entität gefunden wurde, die Ursache für die Erkennung sowie das Datum der Erkennung und der Registrierungstyp.



- **BEREINIGUNG**

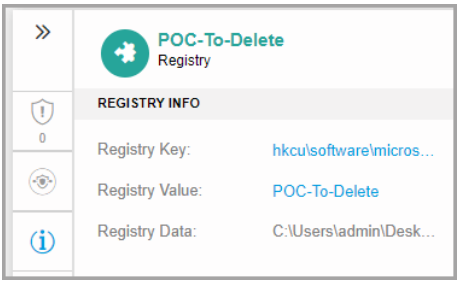
  Hier werden Informationen zu den Aktionen angezeigt, die von GravityZone automatische durchgeführt wurden.



  Bei Registrierungs-Knoten stehen im Abschnitt **BEREINIGUNG** keine Aktionen zur Verfügung, die vom Benutzer durchgeführt werden könnten.

- **REGISTRIERUNGS-INFO**

  Hier werden Details zum jeweiligen Registrierungs-Knoten angezeigt, z. B. Schlüssel, Wert und Daten.

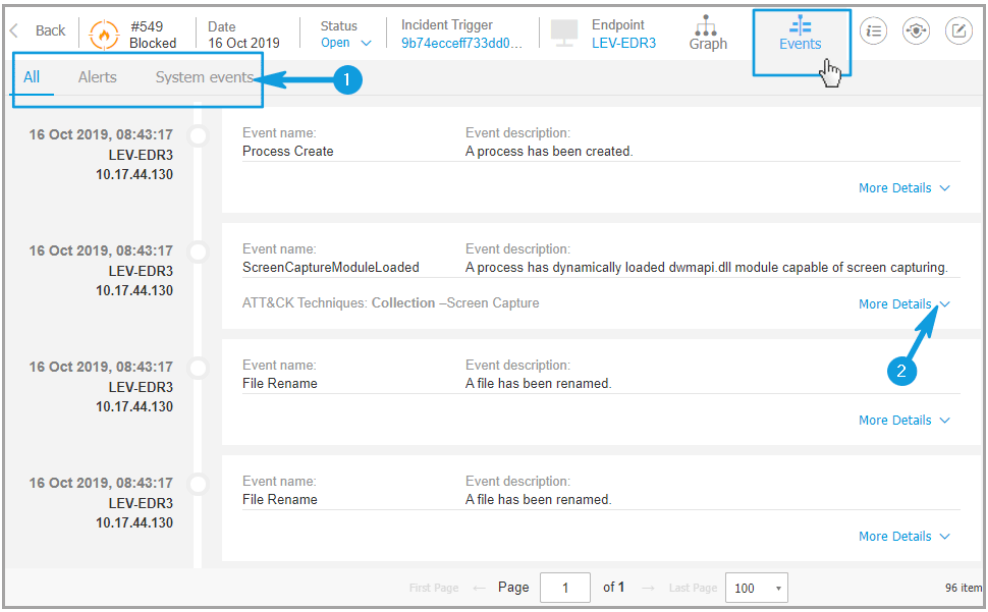


Auf den Schlüssel oder den Wert können Sie klicken, um ihn in die Zwischenablage zu kopieren und an anderer Stelle einfügen zu können.

Ereignisanzeige

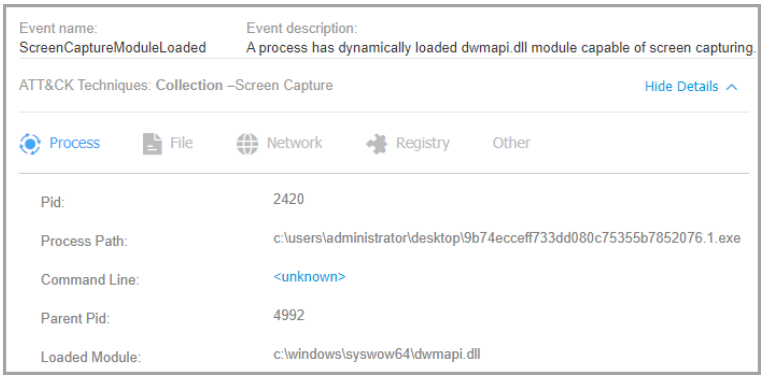
Im Reiter **Ereignisanzeige** können Sie einsehen, welche Abfolge von Ereignissen den aktuell untersuchten Vorfall ausgelöst hat. In diesem Fenster werden die korrelierten Systemereignisse und Warnmeldungen angezeigt, die von GravityZone-Technologien wie EDR,Network Attack Defense, Anomalieerkennung, Erweiterter Exploit-Schutz oder Windows Antimalware Scan Interface (AMSI) erkannt wurden.

Für jedes komplexe Ereignis gibt es eine detaillierte Beschreibung, die erläutert, was gefunden wurde und was passieren kann, wenn das Artefakt für schädliche Zwecke eingesetzt wird (in Übereinstimmung mit den aktuellen MITRE-Techniken und -Taktiken).



Ereignisreiter

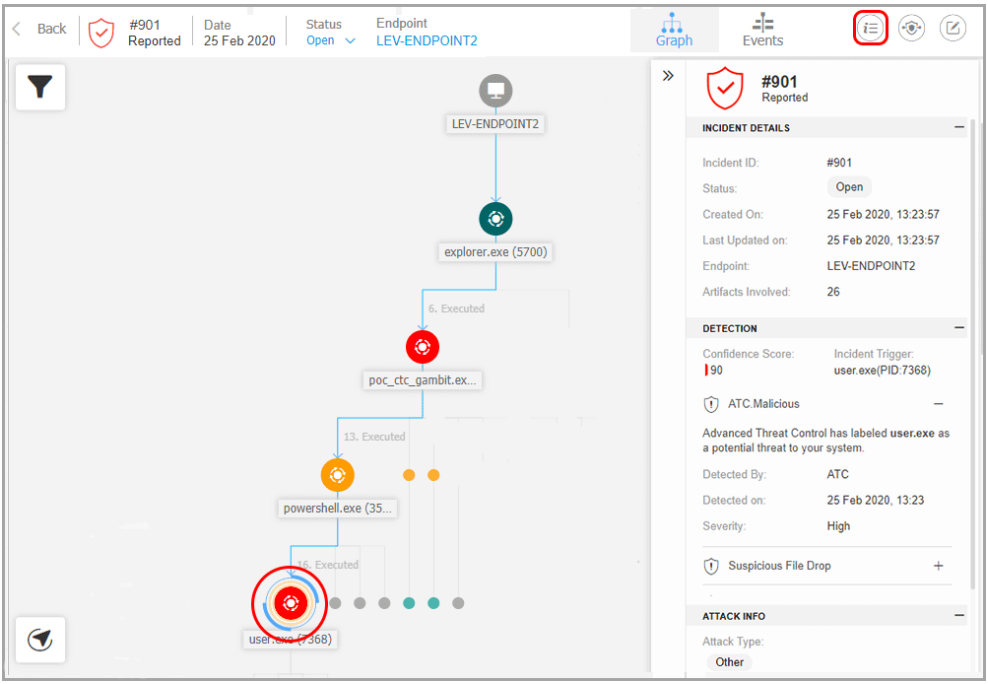
1. Verwenden Sie die Filteroptionen, um alle Ereignisse bzw. entweder nur Systemereignisse oder komplexe Ereignisse (Warnmeldungen) anzuzeigen.
2. Klicken Sie auf die Schaltfläche **Mehr ...**, um die einzelnen Ereignisse zu erweitern und auf zusätzliche Informationen zuzugreifen.



Vorfallsinformationen

In diesem Bereich finden Sie reduzierbare Abschnitte mit Details wie Vorfalls-ID, aktueller Zustand, Zeitstempel der Erstellung und letzten Aktualisierung, Anzahl der beteiligten Artefakte, Name des Auslösers und Beschreibung sowie Angriffsinformationen.

Von diesem Abschnitt aus können Sie den erweiterten Vorfall aufrufen, an dem dieser Endpunktvorfall beteiligt ist, vorausgesetzt, es gibt einen solchen Vorfall.

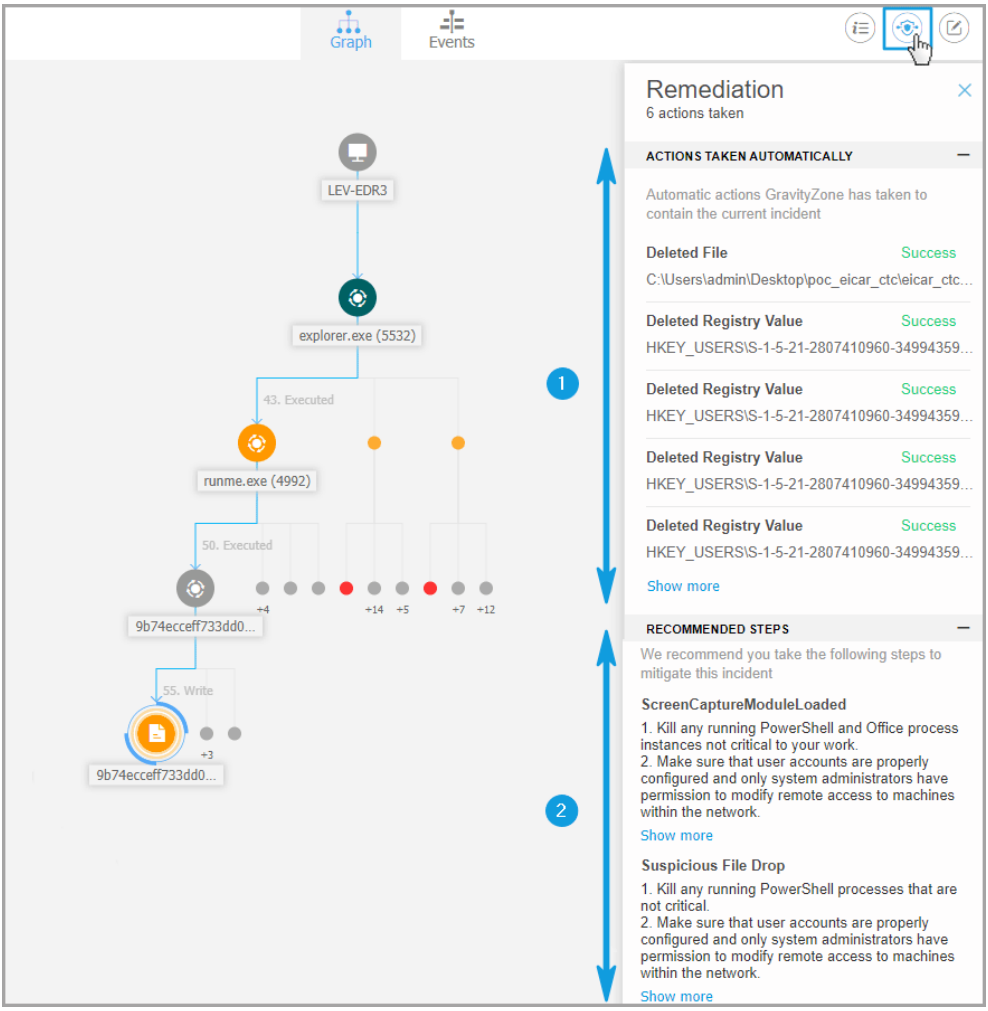


Vorfallsinformationen

Dieser Bereich zeigt auch die Warnmeldungen an, die für das Element gefunden wurden, das den Vorfall ausgelöst hat.

Bereinigung

Im Bereich **Bereinigung** finden Sie aufschlussreiche Informationen darüber, welche Abhilfemaßnahmen GravityZone automatisch ergriffen hat, wenn Angriffe von Technologien wie Advanced Threat Control (ATC), HyperDetect oder dem Malware-Schutz blockiert wurden. Hier finden Sie zudem empfohlene Schritte, mit denen Sie den Vorfall beheben und das Sicherheitsniveau Ihres Systems verbessern können.



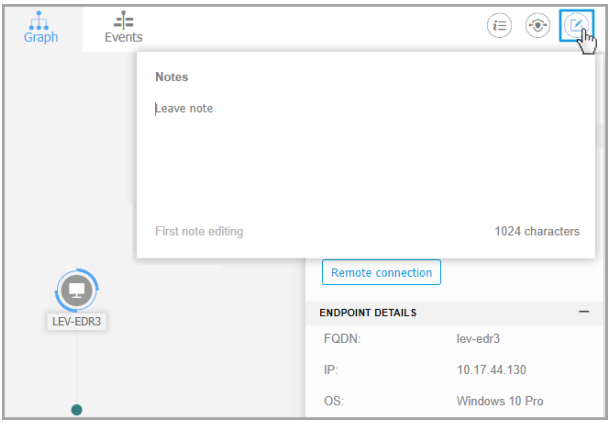
Bereinigung

1. Von GravityZone automatisch ergriffene Aktionen.
2. Empfehlungen zur weiteren Behebung des Vorfalls und zur Verbesserung der Sicherheit.

Beachten Sie
Die empfohlenen Schritte beziehen sich auf die Warnmeldungen, die auf dem Knoten gefunden wurden, der das untersuchte Ereignis ausgelöst hat.

Notizen

Im Bereich **Notizen** können Sie eigene Notizen hinzufügen, um aktuelle Änderungen nachzuverfolgen und die Delegation von Verantwortlichkeiten für einen Vorfall zu erleichtern.

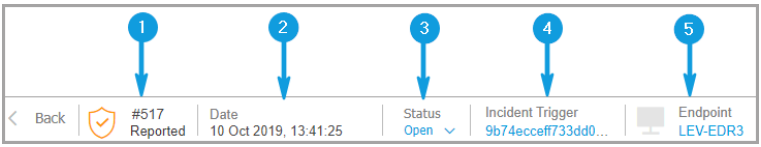


Zwischenablage für Notizen

1. Eine neue Notiz fügen Sie hinzu, indem Sie auf die Schaltfläche **Notizen** klicken und dann im neuen Fenster Ihre Notiz eingeben.
2. Die Länge der Notiz ist auf 2048 Zeichen beschränkt.

Vorfallstatusleiste

Die Vorfallstatusleiste enthält Sicherheitsereignis-Tags, über die Sie wichtige Informationen zu den beteiligten Netzwerkendpunkten finden können.



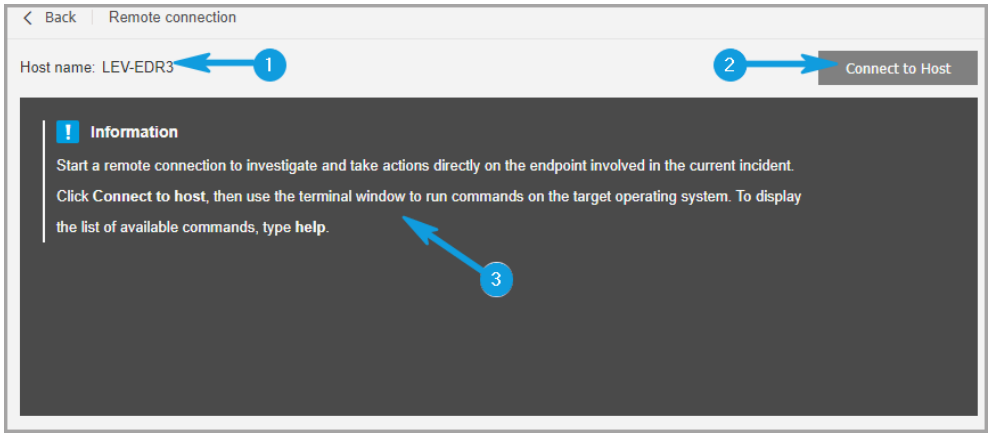
Vorfallstatusleiste

1. Vorfalls-ID - Die ID-Nummer des untersuchten Vorfalls bzw. des blockierten und gemeldeten Vorfalls.
2. Zeitstempel der Erkennung - Das Datum und die Uhrzeit, zu der der Vorfall ausgelöst wurde.
3. Vorfallstatus - Der aktuelle Status des Vorfalls.
4. Vorfalls-Auslöser - Name des Elements, das den Vorfall generiert hat.
5. Endpunkt - Name des Zielendpunkts.

Mit einem Klick auf die Schaltfläche **Zurück** gelangen Sie zurück zur Hauptseite **Vorfälle**.

Remote-Verbindung

Über diesen Reiter können Sie eine Remote-Verbindung zu dem am aktuellen Vorfall beteiligten Endpunkt herzustellen und eine Reihe von benutzerdefinierten Shell-Befehlen direkt auf dem Betriebssystem auszuführen, um die Bedrohung sofort zu unterbrechen oder Daten für die weitere Untersuchung zu sammeln.



Der Reiter Remote-Verbindung

Im Reiter **Remote-Verbindung** finden Sie die folgenden Elemente:

1. Name des Endpunkts, der an dem aktuellen Sicherheitsereignis beteiligt ist.
2. Schaltfläche zur Steuerung der Remote-Verbindung (Verbinden / Trennen)
3. Das Terminalfenster

Voraussetzungen für eine Terminalsitzung

- Die auf dem Endpunkt installierte Version des Bitdefender-Agenten unterstützt die Funktion Remote-Verbindung.
- Der Endpunkt muss eingeschaltet und online sein.
- Der Endpunkt muss über ein Windows-Betriebssystem verfügen.
- GravityZone ist zur Kommunikation mit dem Endpunkt in der Lage.
- Ihr GravityZone-Benutzerkonto muss über Verwaltungsberechtigungen für den Zielendpunkt verfügen.

Eine Remote-Verbindung herstellen

So funktioniert die Remote-Verbindung:

1. Starten Sie die Live-Sitzung, indem Sie auf die Schaltfläche **Verbindung mit Host herstellen** klicken.

Der Verbindungsstatus wird neben dem Endpunktnamen angezeigt.

Wenn die Verbindung fehlschlägt, wird im Terminalfenster eine Fehlermeldung angezeigt.

Beachten Sie
Sie können maximal fünf Terminalsitzungen mit dem gleichen Endpunkt gleichzeitig eröffnen.

2. Nach dem Aufbau der Verbindung zeigt das Terminal die Liste der verfügbaren Befehle und deren Beschreibung an. Geben Sie den gewünschten Befehl im Terminalfenster ein und drücken Sie danach die `Eingabetaste`.

   Um mehr über einen Befehl zu erfahren, geben Sie `help` gefolgt von dem Befehlsnamen ein (z. B. `help ps`).

3. Das Terminal zeigt die Befehlsausgabe an, wenn der Befehl erfolgreich ausgeführt wurde.

   Wenn der Endpunkt die Befehlsausführung nicht beendet, wird der Befehl verworfen.

   Der Befehlsverlauf wird im Terminalfenster protokolliert. Sie können jedoch die zuvor eingegebenen Befehle durch Drücken der Pfeiltasten anzeigen.

4. Klicken Sie zum Beenden der Verbindung auf die Schaltfläche **Sitzung beenden**.

   Die Terminalsitzung läuft nach fünf Minuten Inaktivität automatisch ab.

   Wenn Sie den Reiter **Remote-Verbindung** verlassen, während Sie mit einem Endpunkt verbunden sind, wird die Terminalsitzung ebenfalls beendet.

Befehle für die Terminalsitzung

Die EDR-Terminalsitzungsbefehle sind benutzerdefinierte Shell-Befehle, die plattformunabhängig sind und eine generische Syntax verwenden. Nachfolgend finden Sie die Liste der verfügbaren Befehle, die Sie auf den Endpunkten während einer Terminalsitzung verwenden können:

- `ps`
  - **Beschreibung**: Zeigt Informationen über die aktuell laufenden Prozesse auf dem Zielendpunkt an, so z. B. Prozess-ID (PID), Name, Pfad oder Speicherauslastung.

  - **Syntax**: `ps`
  - **Aliase**: `tasklist`
  - **Parameter**: -

- `kill`
  - **Beschreibung**: Beendet einen laufenden Prozess oder eine Anwendung auf dem Zielendpunkt über die jeweilige PID. Verwenden Sie den Befehl `ps/tasklist`, um die PID zu abzurufen.
  - **Syntax**: `kill [PID]`
  - **Aliase**: -
  - **Parameter**: `[PID]` - die ID eines Prozesses auf dem Zielendpunkt.
- `ls (dir)`
  - **Beschreibung**: Zeigt Informationen über alle Dateien und Ordner im angegebenen Verzeichnis an, wie Name, Typ, Größe und Änderungsdatum. Ermöglicht die Angabe des Pfads über Platzhalter. Zum Beispiel:

    `C:\Users\admin\Desktop\s*` alle Inhalte des Desktop-Ordners, die mit "s" beginnen

    `C:\Users\publ??` listet alle Inhalte des angegebenen Pfades mit beliebigen letzten zwei Buchstaben auf.
  - **Syntax**: `ls [path]`
  - **Aliase**: `dir`
  - **Parameter**: `[Path]` - den Pfad zu einer Datei oder einem Ordner auf dem Zielendpunkt.
- `rm (del, delete)`
  - **Beschreibung**: Löscht Dateien und Ordner aus dem angegebenen Pfad auf dem Zielendpunkt.
  - **Syntax**: `rm [path]`
  - **Aliase**: `del/delete`

- **Parameter**: `[Path]` - den Pfad zu einer Datei oder einem Ordner auf dem Zielendpunkt.

- `reg query`
  - **Beschreibung**: Gibt alle Informationen (Name, Typ und Wert) für den angegebenen Registrierungsschlüsselpfad zurück.
  - **Syntax**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Aliase**: -
  - **Parameter**:
    - `keypath`- gibt alle Registrierungsschlüsselinformationen aus dem angegebenen Pfad zurück.
    - `/k [keyname]` - filtert die Registrierungsschlüsselergebnisse nach einem bestimmten Schlüsselnamen. Sie können auch Platzhalter (*, ?) verwenden, um nach einem größeren Namensbereich zu filtern.
    - `/v [valuename]` - filtert die Registrierungswerte nach einem bestimmten Wertnamen. Sie können auch Platzhalter (*, ?) im Wertnamen verwenden, um nach einem größeren Namensbereich zu filtern.

- `reg add`
  - **Beschreibung**: Fügt einen neuen Registrierungsschlüssel oder -wert hinzu. Überschreibt einen bereits vorhandenen Registrierungswert. Beim Überschreiben von Registrierungsinformationen müssen Sie alle definierten Parameter angeben.
  - **Syntax**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Aliase**: -
  - **Parameter**:
    - `[keyname]` - der Name des Registrierungsschlüssels.
    - `/v [valuename]` - der Name des Registrierungswerts. Es muss auch mindestens der Parameter /d [data] hinzugefügt werden.
    - `/t [datatype]` - der Datentyp des Registrierungswerts. Sie können einen der folgenden Datentypen hinzufügen:

`REG_SZ`, `REG_MULTI_SZ`, `REG_DWORD`, `REG_BINARY`, `REG_DWORD_LITTLE_ENDIAN`, `REG_LINK`, `REG_FULL_RESOURCE_DESCRIPTOR`, `REG_EXPAND_SZ`

Wenn nicht angegeben, wird der `REG_SZ`-Typ standardmäßig zugeordnet.

Wenn der Typ auf `REG_BINARY` festgelegt wird, werden Registrierungsdaten als Hex-Werte interpretiert.

- `reg delete`
  - **Beschreibung**: Löscht einen Registrierungsschlüssel oder seine Werte..
  - **Syntax**:

    ```
    reg delete [keyname] [/v] [valuename]
    ```

    ```
    reg delete [keyname] [/va]
    ```
  - **Aliase**: -
  - **Parameter**:

    `[keyname]` - löscht einen Registrierungsschlüssel und alle seine Werte.

    `/v [valuename]` - löscht den angegebenen Registrierungswert.

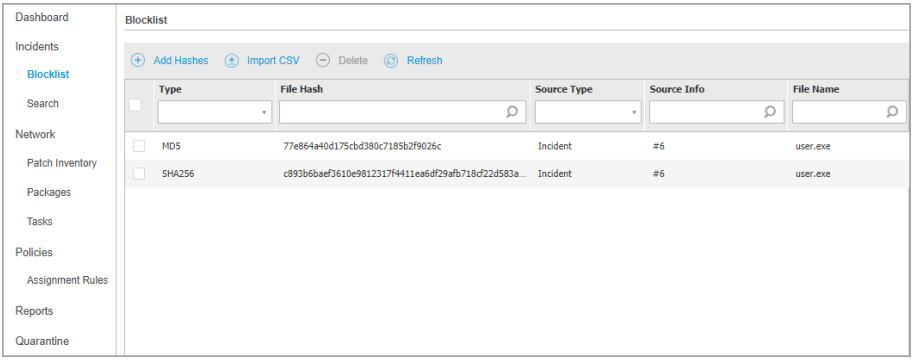
    `/va` - löscht alle Werte des angegebenen Registrierungsschlüssels.
- `cd`
  - **Beschreibung**: Ändert das Arbeitsverzeichnis auf den angegebenen Pfad. Dieser Befehl erfordert als Parameter den Pfad zu einem Laufwerk oder Ordner vom Zielendpunkt aus.
  - **Syntax**: `cd [path]`
  - **Aliase**: -
  - **Parameter**: `[Path]` - den Pfad zu einer Datei oder einem Ordner auf dem Zielendpunkt.
- `hilfe`
  - **Beschreibung**: Ohne Angabe eines Parameters listet help alle verfügbaren Befehle mit einer kurzen Beschreibung auf. Wenn Sie help gefolgt von einem Parameter eingeben, zeigt es die vollständige Syntax dieses Befehls, eine kurze Beschreibung und ein Anwendungsbeispiel an.

- **Syntax**: `help [command]`
- **Aliase**: -
- **Parameter**: Befehlsname (z. B.: `cd, kill, ls, ps`)

- `clear (cls)`
  - **Beschreibung**: Löscht den Inhalt des Terminalfensters und zeigt die Eingabeaufforderung mit dem aktuellen Arbeitsordner an.
  - **Syntax**: `clear`
  - **Aliase**: `cls`
  - **Parameter**: -

9.2. Dateien zur Blockierliste hinzufügen

Im Bereich **Blockierliste** können Sie Objekte nach ihren Hashwerten anzeigen und verwalten. Aktivitätsprotokolle können unter Benutzeraktivitätsprotokoll angezeigt werden.



Blockierliste

Der Datentabelle können Sie die folgenden Details für jedes Objekt entnehmen:

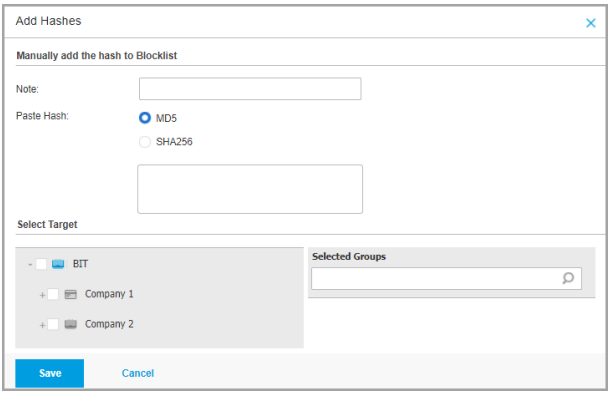
- Dateitypen:
  - MD5
  - SHA256

- Hashwert der Datei
- Quellentyp:
  - Vorfall (EDR)
  - Importieren
  - Manuell
- Quelleninfo
- Dateiname
- Unternehmen

So fügen Sie Hash-Werte zur bestehenden Blockierliste hinzu:

1. Kopieren Sie den Hashwert aus der **Datei-Info**.
2. Wählen Sie zwischen **MD5** und **SHA256** und fügen Sie den Wert in das untere Textfeld ein.

   Sie können bei Bedarf eine Notiz hinzufügen.
3. Klicken Sie auf **Speichern**.

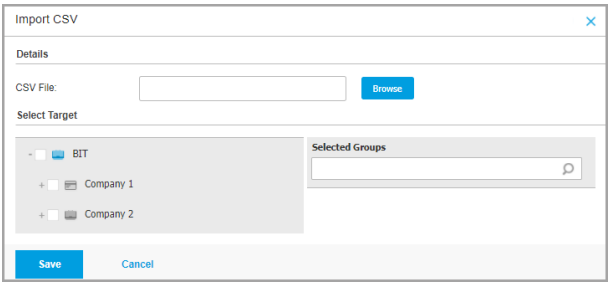


Fenster zum Hinzufügen des Hashwerts

Wichtig
Der **Vorfall-Sensor** hindert jede Binärdatei, deren Hash-Wert zur **Blockierliste** hinzugefügt wurde, daran, einen Prozess zu starten.

Importieren von Hash-Datensätzen in die bestehende Blockierliste. Gehen Sie zum Importieren einer CSV-Datei folgendermaßen vor:

1. Klicken Sie auf **CSV importieren**.
2. Suchen Sie nach der entsprechenden CSV-Datei und klicken Sie auf **Speichern**.



Fenster für den CSV-Import

Sie können auch lokale CSV-Dateien von Ihrem Gerät in die Seite **Blockierliste** importieren. Stellen Sie jedoch zunächst sicher, dass Ihre CSV gültig ist.

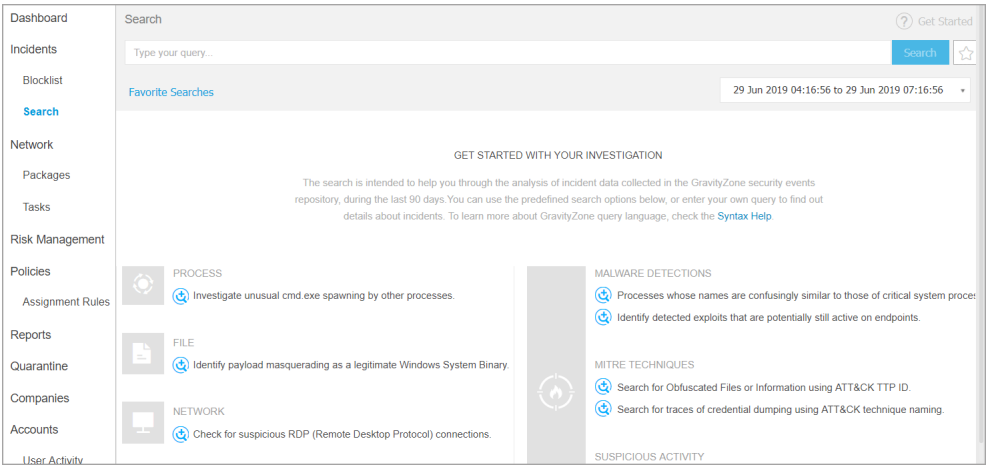
Um eine gültige CSV-Datei für den Import zu erstellen, müssen Sie die ersten drei Spalten mit den folgenden Daten füllen:

1. In der ersten Spalte der CSV-Datei muss der Hash-Typ angegeben sein: entweder `md5` oder `sha256`.
2. Die zweite Spalte muss die entsprechenden hexadezimalen Hash-Werte enthalten.
3. Die dritte Spalte kann optionale Informationen zur Zeichenfolge enthalten, die sich auf die Spalte **Quelleninfo** auf der Seite **Blockierliste** beziehen.

Beachten Sie
Informationen, die sich auf die anderen Spalten auf der Seite **Blockierliste** beziehen, werden beim Import der CSV-Datei automatisch eingefügt.

9.3. Sicherheitsereignisse durchsuchen

Auf der Seite **Suchen** können Sie vergangene Ereignisse nach komplexen Kriterien durchsuchen.



Suchseite

Um die Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie mithilfe der in GravityZone eingebauten Abfragesprache Abfragen erstellen.

Auf der Seite **Suche** finden Sie die folgenden Optionen:

- Eine Suchleiste zur Eingabe von Abfragen, die beim Anklicken die Liste der Abfragebegriffe nach Kategorien anzeigt, sowie einen Assistenten für die automatische Vervollständigung.
- Die Möglichkeit für weitere Suchen Suchfavoriten zu speichern.
- Filteroptionen nach Datum und Uhrzeit.
- Den Abschnitt **Erste Schritte** mit einem Link zur Syntaxhilfe für die Abfragesprache.
- Vordefinierte Abfragen, entwickelt für nützliche Suchvorgänge nach Sicherheitsereignissen.

9.3.1. Die Abfragesprache

Die Abfragesprache definiert das Vokabular (Felder und Operatoren) und die Syntax, mit der Sie die Abfragen erstellen können. Sie werden im Folgenden beschrieben.

Über den Link **Syntaxhilfe** finden Sie im Reiter **Abfragesprache** weitere Informationen.

Felder

Das Abfragefeld ist ist dasselbe wie das Feld in der GravityZone-Datenbank. Felder stehen z. B. für Dateipfade, Datei-Hashes, Hostnamen oder Domainnamen.

Jedes Feld kann einen oder auch mehrere Werte beinhalten, wobei jeder Wert den Zustand des Feldes zu einer bestimmten Zeit darstellt. Werte können je nach Art des Feldes unterschiedliche Datentypen sein.

Operatoren

Mit Operatoren können Sie Beziehungen zwischen Feldern herstellen um Suchkriterien zu erstellen. Die folgenden Operatoren stehen zur Verfügung:

Operator	Beispiel	Beschreibung
`:`	`fieldCategory.option: value1`	Vergleicht den Wert des Abfragefeldes mit den Werten desselben Feldes in der Datenbank.
`" "`	`fieldCategory.option: "value1 value2"`	Zeichenfolgen, die innerhalb von Anführungszeichen stehen, werden als eine Einheit behandelt.
`( )`	`fieldCategory1.option: value1 UND (fieldCategory2.option: value2 OR fieldCategory3.option: value3)`	Fasst Abfrageterme zu einer Gruppe zusammen.
`AND`	`fieldCategory1.option: value1 UND fieldCategory2.option: value2`	Zeigt Ergebnisse an, die alle gewählten Abfragebedingungen erfüllen.
`oder`	`fieldCategory1.option: value1 ODER fieldCategory2.option: value2`	Zeigt Ergebnisse an, die beliebig viele der gewählten Abfragebedingungen erfüllen.

Operator	Beispiel	Beschreibung
`UND NICHT`	`fieldCategory1.option: value1 UND NICHT fieldCategory2.option: value2`	Dieser Operator eignet sich für komplexe Abfragen und liefert neben allen anderen Bedingungen Ergebnisse, die nicht dem angegebenen Begriff entsprechen.
`_exists_`	`_exists_: fieldCategory.option`	Bringt Ergebnisse, die das angegebene Feld beinhalten.
`-`	`fieldCategory.option: -value`	Mit dem Minuszeichen (-) können Werte von den Ergebnissen ausgeschlossen werden.
`?`	`fieldCategory.option: ???_file.path`	Mit einem Fragezeichen (?) kann ein beliebiges Zeichen im Feldwert ersetzt werden.
`*`	`fieldCategory.option: file.*`	Mit einem Asterisk (*) kann ein beliebiger Feldwert ersetzt werden.

Syntax der Abfragen

Eine Abfrage ist eine logische Bedingung (oder Folge von Bedingungen, die mithilfe von Operatoren verknüpft sind), deren Ergebnisse Ereignisse aus der EDR-Datenbank sind.

Alle Bedingungen müssen sich auf Felder beziehen. Bei einigen Bedingungen muss ein Wert mit angegeben werden, bei anderen nicht. Wenn z. B. nur danach gefragt wird, ob ein Feld in den Ereignisdetails existiert, wird kein Wert benötigt.

Abfragen haben von ganz simpel bis ganz komplex eine große Bandbreite. Komplexe Abfragen können verschachtelt sein (d. h. Abfragen innerhalb einer Abfrage beinhalten).

Eine gültige Feldsyntax besteht aus der Feldkategorie, gefolgt von einer der Optionen im Abschnitt **Abfragesprache** und dem entsprechenden Wert: `fieldCategory.option: value`.

`file.path: "%system32%\com\svchost.exe"` zum Beispiel ist eine relativ einfache Abfrage, die alle Ereignisse durchsucht, die `%system32%\com\svchost.exe` beinhalten, und besteht aus:

- Einer Pflichtfeldkategorie und der zugehörigen Option (getrennt durch einen Punkt): `file.path`
- einem Operator: dem Doppelpunkt (:) – um den Feldwert zu vergleichen
- Dem gesuchten Wert: `%system32%\com\svchost.exe`
- Anführungszeichen (" "), da der Wert Sonderzeichen wie <\> und <.> enthält.

9.3.2. Abfragen durchführen

So führen Sie eine Abfrage durch:

1. Geben Sie die Zeichenfolge der Abfrage in das Feld ein.

   Durch Anklicken des Feldes **Suche** wird die Liste der Suchbegriffe nach Kategorien geordnet angezeigt. Wählen Sie den Begriff aus, mit dem Sie die Erstellung Ihrer Abfrage beginnen möchten.

   Während der Eingabe unterstützt das Control Center Sie mit der Autovervollständigungsfunktion. Mithilfe der Pfeiltasten können Sie einen Vorschlag auswählen und ihn mit der **Enter**-Taste in die Abfrage einfügen.

   Weitergehende Hilfethemen finden Sie über den Link **Syntaxhilfe**.

   Beachten Sie
   Mithilfe verschachtelter Abfragen können Sie komplexe Suchanfragen stellen.

2. Klicken Sie auf das Zeitfeld, um Ereignisse innerhalb eines Zeitrahmens zu filtern.

   Wichtig
   Die Daten zu Ereignissen werden standardmäßig 7 Tage gespeichert. Um zusätzlichen Speicherplatz zu erhalten, wenden Sie sich bitte an Ihren zuständigen Vertriebsmitarbeiter, um Ihre Lösung mit einem Add-on für 30, 90 oder 180 Tage **Datenspeicherung** zu erweitern.

   Sie haben mehrere Möglichkeiten, den Suchzeitraum festzulegen:

   - Ein bestimmtes Datum.

     Wählen Sie im Reiter **ab** des Kalenders ein Datum.
   - Ein bestimmter Zeitraum.

     a. Legen Sie im Reiter **ab** des Kalenders das Startdatum fest.

b. Legen Sie im Reiter **Bis** das Enddatum fest.

- Ein jüngerer Zeitraum aus der verfügbaren Auswahl.
- Klicken Sie auf **OK**.

3. Klicken Sie auf **Suche**, oder drücken Sie **Eingabe**.

   Die passenden Ergebnisse werden samt der zugehörigen Details unter Ihrer Abfrage angezeigt.

Wichtig

Wenn Sie die Abfrage `detections.detection_type` im Feld *Suche* durchführen, müssen Sie in Control Center einen ganzzahligen Wert von 1 bis 15 eingeben (d. h. `detections.detection_type:1`).

Jeder eingegebene Wert entspricht einem bestimmten Erkennungstyp:

a. `detections.detection_type:1` - Erkennung mit Advanced Threat Control

b. `detections.detection_type:2` - Erkennung durch statische Malware-Schutz-Engines

c. `detections.detection_type:3` - Erkennung durch HyperDetect

d. `detections.detection_type:4` - Benachrichtigung über verdächtige Ereignisse durch Advanced Threat Control

e. `detections.detection_type:5` - Erkennung von Angriffstypen, die von HyperDetect gemeldet wurden

f. `detections.detection_type:6` - Erkennung durch Befehlszeilen-Scanner für Malware-Schutz

g. `detections.detection_type:7` - Erkennung mit Cross Technologies Correlation

h. `detections.detection_name:8` - Erkennung mit Network Attack Defense

i. `detections.detection_type:9` - Erkennung von Angriffstypen, die nicht von HyperDetect gemeldet wurden

j. `detections.detection_type:10` - Erkennung durch eine dynamische Analyse in einer geschlossenen Umgebung mit Sandbox Analyzer

k. `detections.detection_type:11` - Erkennung durch Arbeitsspeicherpuffer-Register-Scan

l. `detections.detection_type:12` - URL-Erkennung

m. `detections.detection_type:13` - Erkennung mit Advanced Anti-Exploit

n. `detections.detection_type:14` - Erkennung durch Analyse des Benutzerverhaltens

o. `detections.detection_type:15` - Erkennung durch Malware-Scan auf der Benutzeroberfläche

p. `detections.detection_type:16` - technologieübergreifender Korrelationsfund auf Grundlage von maschinellem Lernen

Das Control Center kann bis zu 10.000 Ereignisse anzeigen. Wenn die Abfrage mehr als 10.000 Ergebnisse liefert, wird eine entsprechende Meldung angezeigt. In solchen Fällen sollten Sie Ihre Abfrage stärker einschränken.

9.3.3. Suchfavoriten

Viele Abfragen sind lang, und einige sind sehr aufwändig zu erstellen oder schwierig zu merken. Anstatt die Abfragen in einer Datei zu speichern und bei Bedarf nach GravityZone zu kopieren, können Sie sie für schnellen Zugriff direkt in GravityZone speichern.

So speichern Sie eine Abfrage:

1. Geben Sie die Zeichenfolge in das Feld **Suche** ein.
2. Klicken Sie rechts neben dem Feld **Suche** auf das ☆-Symbol.
3. Geben Sie dem Lesezeichen einen Namen.
4. Klicken Sie auf **Hinzufügen**.

Wenn Sie Ihre gespeicherten Abfragen anzeigen möchten, klicken Sie unter dem **Abfrage**-Feld auf den Link **Suchfavoriten**.

Hier haben Sie drei Möglichkeiten:

- Die Abfrage durchführen.
- Den Namen der Abfrage ändern.
- Die Abfrage löschen.

So führen Sie eine gespeicherte Abfrage durch:

1. Klicken Sie auf den Link **Suchfavoriten**.
2. Wählen Sie die gewünschte Abfrage.

   Die gespeicherte Zeichenfolge wird in das Feld **Suche** eingefügt.

   Beachten Sie
   Ändern Sie die Abfrage bei Bedarf ab. Zusätzlich können Sie die neue Suchanfrage in Ihren Suchfavoriten speichern.

3. Schränken Sie die Suche mithilfe der Unternehmens- und Kalenderfilter ein.
4. Klicken Sie auf **Suchen**.

Wenn Sie etwas an einer gespeicherten Abfrage ändern möchten, bewegen Sie den Mauszeiger auf die Abfrage. Es werden weitere Optionen angezeigt.

- Klicken Sie auf das **Bearbeiten**-Symbol, um die Abfrage umzubenennen.
- Klicken Sie auf das **Löschen**-Symbol, wenn Sie die Abfrage nicht mehr benötigen.

9.3.4. Vordefinierte Abfragen

Auf der Seite **Suche** finden Sie Beispiele für komplexe Suchabfragen speziell für die Untersuchung von Sicherheitsereignissen.

Vordefinierte Abfragen sind nach Kategorien von Sicherheitsuntersuchungen geordnet.

So können Sie eine vordefinierte Abfrage starten:

- Klicken Sie auf das -Symbol neben der Beschreibung der vordefinierten Abfrage.
- Der Suchausdruck wird automatisch in der Leiste **Suche** angezeigt. Geben Sie die spezifischen Details für die Suchbegriffe ein.
- Klicken Sie auf die Schaltfläche **Suche**, um die Abfrage zu starten.

Beachten Sie
Sie können von der Seite **Suche** jederzeit zu den Optionen unter **Erste Schritte** zurückkehren, indem Sie auf den Link **Erste Schritte** oben rechts auf der Seite klicken.

9.4. Benutzerdefinierte Regeln

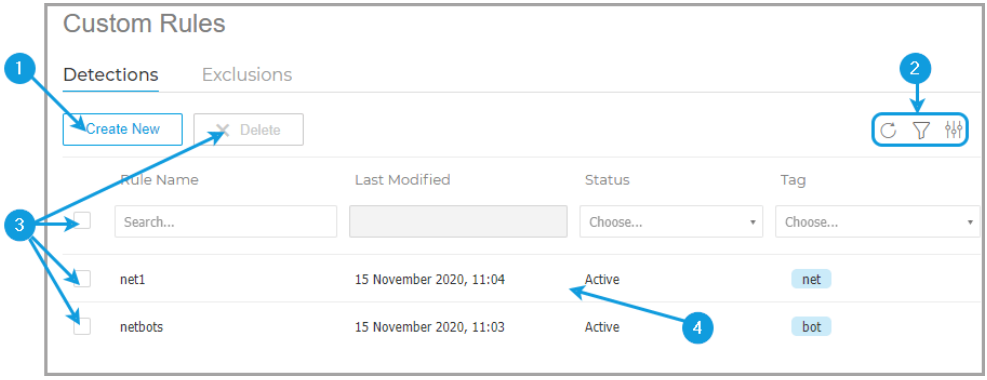
Auf der Seite **Benutzerdefinierte Regeln** können Sie benutzerdefinierte Regeln erstellen und verwalten. Hier können Sie festlegen, welche Verhaltensweisen einen Vorfall auslösen bzw. erlaubt sind.

Diese EDR-Funktion umfasst zwei Hauptkategorien:

- Funde
- Ausschlüsse

9.4.1. Funde

Im Reiter **Funde** können Sie benutzerdefinierte Erkennungsregeln erstellen und verwalten, um bestimmte Verhaltensweisen in Ihrer Umgebung festzulegen, die in der Folge als gültiger Fund gelten und einen entsprechenden Vorfall auf der Seite Vorfälle generieren.



Reiter Funde

1. Klicken Sie auf die Schaltfläche **Neu anlegen**, um eine neue benutzerdefinierte Erkennungsregel anzulegen. Weitere Einzelheiten finden Sie im Abschnitt Erstellen von benutzerdefinierten Ausschlussregeln.
2. Über die folgenden Schaltflächen können Sie die Anzeige anpassen:
   - Über die Schaltfläche **Spalten ein-/ausblenden** können Sie einzelne Filterspalten hinzufügen oder entfernen.

Die Seite wird automatisch mit den Karten neu geladen, deren Daten zu den hinzugefügten Spalten passen.

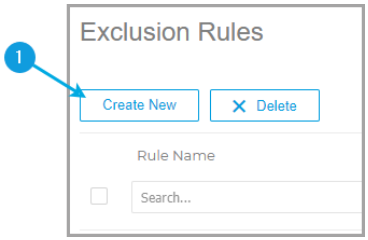
Über die Schaltfläche **Zurücksetzen** im Klappmenü **Spalten ein-/ausblenden** können Sie die Filter jederzeit zurücksetzen.

- Über die Schaltfläche **Filter ein-/ausblenden** können Sie die Filterleiste ein- oder ausblenden.
- Über die Schaltfläche **Neu laden** können Sie die Liste neu laden.

3. Markieren Sie das Sammelkästchen oder die einzelnen Kästchen der Regeln, um sie auszuwählen, und klicken Sie auf **Löschen**, um sie aus der Liste zu entfernen.
4. Klicken Sie auf eine Regel in der Liste, um den Detailbereich aufzuklappen, die Regeldetails anzuzeigen und sie bei Bedarf zu aktualisieren oder zu löschen. Weitere Einzelheiten finden Sie im Detailfenster für Erkennungsregeln.

Erstellen von benutzerdefinierten Erkennungsregeln

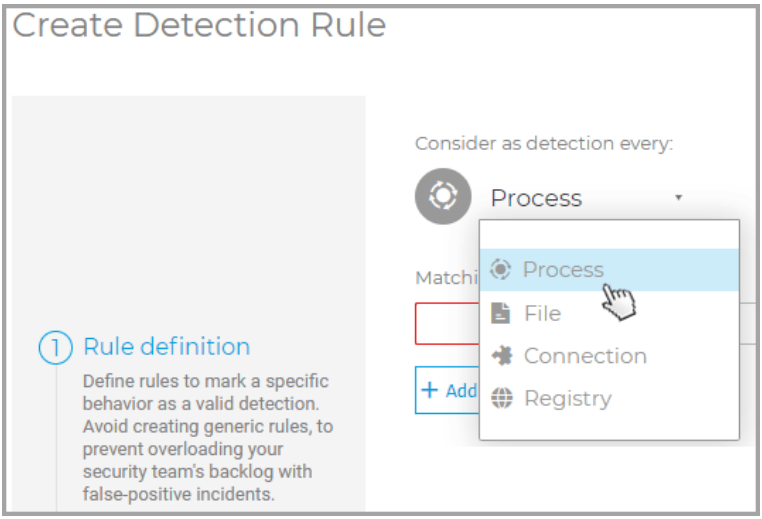
Klicken Sie auf **Neu anlegen**, um eine benutzerdefinierte Erkennungsregel zu erstellen,



Erstellen einer neuen Erkennungsregel

Die Seite **Erkennungsregel erstellen** mit dem Abschnitt **Regeldefinition** wird angezeigt. Hier können Sie mit der Bearbeitung der Regel beginnen:

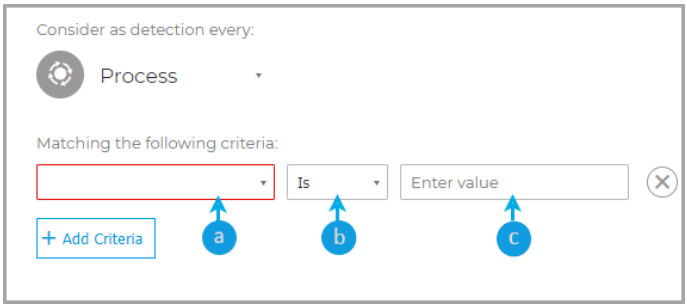
1. Wählen Sie aus, welchen Elementtyp Sie in die Ausschlussregel aufnehmen möchten.



Zur Auswahl stehen:

- Prozess
- Datei
- Verbindung
- Registrierung

2. Jeder Elementtyp hat spezifische Übereinstimmungskriterien, die Sie aus dem Dropdown-Menü auswählen können:



a. Wählen Sie eine der verfügbaren Kriterienoptionen aus.

b. Wählen Sie die Art der Beziehung zwischen den Übereinstimmungskriterien und den entsprechenden Wert aus:

   - **Ist** - umfasst alle Vorfälle mit Objekten, die genau dem im Wertfeld eingegebenen Wert entsprechen.
   - **Enthält** - umfasst alle Vorfälle mit Objekten, die den im Wertfeld eingegebenen Wert enthalten (z. B. Platzhalter, Dateierweiterungen usw.).

     Wichtig
     Die Verwendung von Platzhaltern bei der Erstellung einer Erkennungsregel erhöht das Risiko, dass sie zu allgemein gehalten wird, was die Wahrscheinlichkeit erhöht, dass Sie zu viele Fehlalarme abarbeiten müssen.

   - **Ist eines von** - umfasst alle Vorfälle mit Objekten, die mit einem der im Wertfeld eingegebenen Werte übereinstimmen (der Operator **ODER** wird zwischen den eingegebenen Werten angewendet).

c. Geben Sie den spezifischen Wert für jedes Kriterium ein.

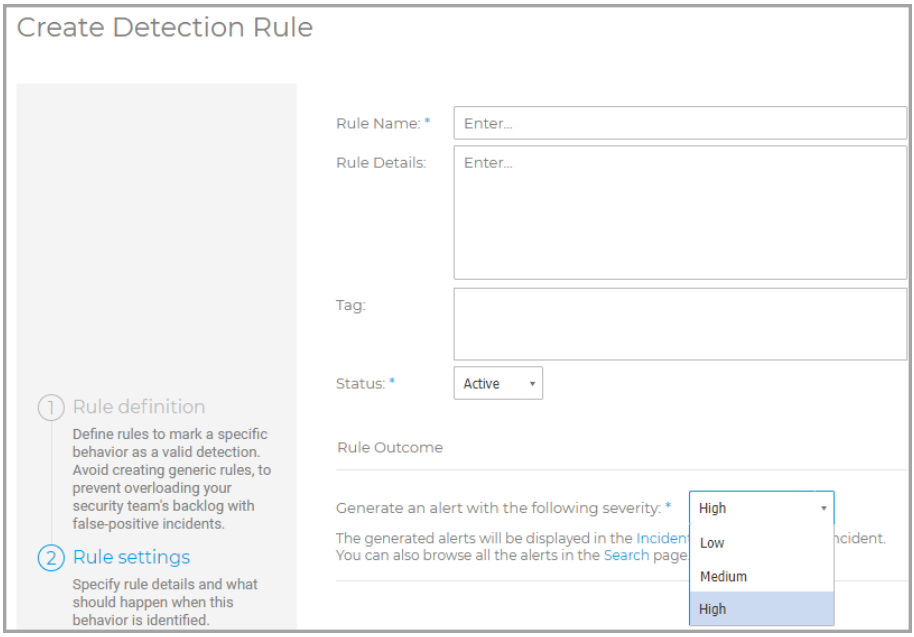
   Beachten Sie
   Wenn Sie mehrere Werte für ein Kriterium eingeben (bei Verwendung der Bedingung **Ist eine von**), müssen Sie nach jedem Wert **Eingabe** drücken, um die Aktion abzuschließen.

3. Klicken Sie auf **Kriterien hinzufügen**, um der Regel ein neues Kriterium hinzuzufügen.

Beachten Sie
Die Regel löst Vorfälle aus, die alle definierten Kriterien enthalten (der Operator **UND** wird zwischen mehreren hinzugefügten Kriterien angewendet).

4. Nachdem alle Kriterien definiert sind, klicken Sie auf **Nächster Schritt**.

   Der Abschnitt **Regeleinstellungen** wird angezeigt, wo Sie die Regeldetails ausfüllen müssen.



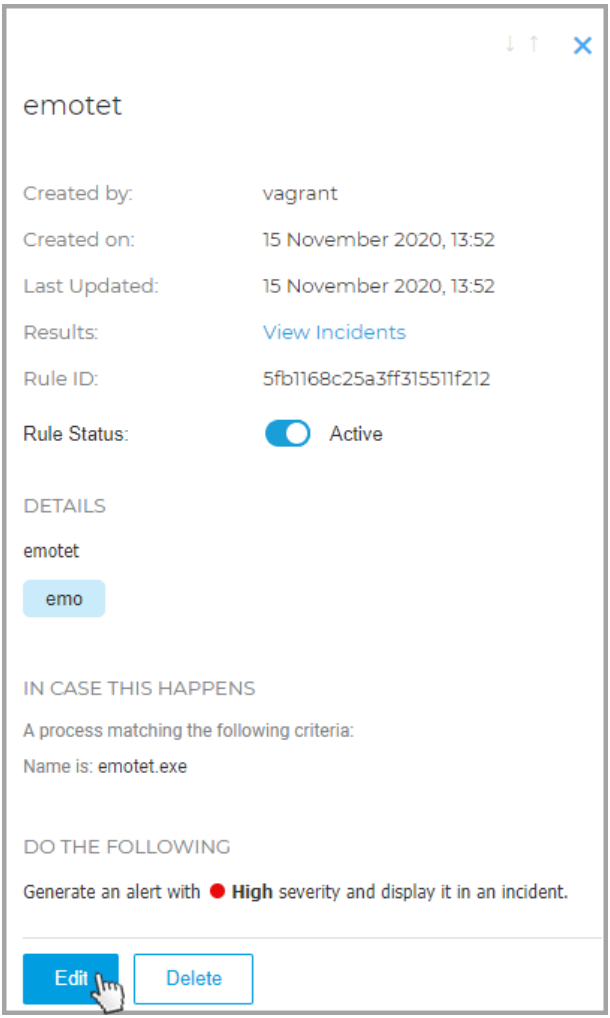
5. Benennen Sie die neue Regel im Feld **Regelname**. Dies ist ein Pflichtfeld.
6. Fügen Sie eine kurze Beschreibung der Regel im Textbereich **Regeldetails** hinzu.
7. Fügen Sie für diese Regel spezifische Tags im Feld **Tag** hinzu, um die Gruppierung und Verwaltung von Regeln zu erleichtern.
8. Legen Sie den Regelstatus über das Dropdown-Menü **Status** auf Aktiv oder Inaktiv fest.

9. Legen Sie den Schweregrad der durch diese Regel ausgelösten Warnmeldungen im Dropdown-Menü auf Niedrig / Mittel / Hoch fest.
10. Klicken Sie auf **Regel erstellen**, um die Erstellung der benutzerdefinierten Ausschlussregel abzuschließen.

    Sie finden die neue Regel im Reiter **Funde**.

Detailfenster für Erkennungsregeln

Im Bereich **Regeldetails** finden Sie detaillierte Informationen über die ausgewählte Regel, einschließlich Erstellungsdatum und Ersteller, Datum der letzten Aktualisierung, eindeutige ID und Status sowie einen Link zu einer Liste von Ereignissen, die den Kriterien der Regel entsprechen. Hier finden Sie zudem eine Beschreibung der Regel, die zugehörigen Tags, die enthaltenen Übereinstimmungskriterien und das Ergebnis der Regel.

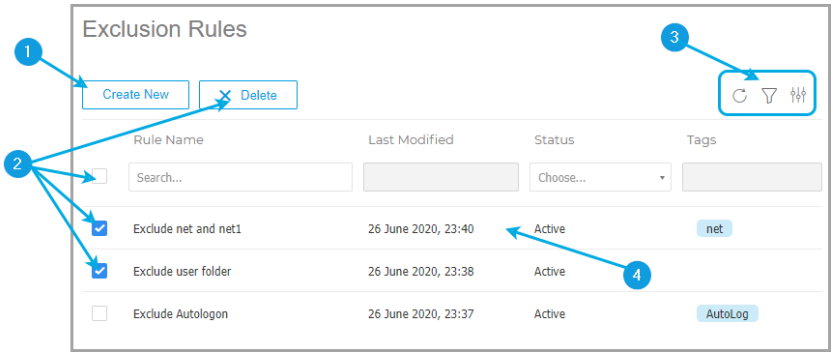


Bereich Regeldetails

- Klicken Sie auf **Bearbeiten**, um die Seite **Erkennungsregel erstellen** aufzurufen, auf der Sie die Regeldefinition aktualisieren können.
- Klicken Sie auf **Löschen**, um die Ausschlussregel aus der Liste zu entfernen.

9.4.2. Ausschlüsse

Im Reiter **Ausschlüsse** können Sie benutzerdefinierte Ausschlussregeln erstellen und verwalten, um Vorfälle auszuschließen, die Sie für Ihr Unternehmen als nicht relevant einstufen und die sonst von EDR auf der Seite Vorfälle gekennzeichnet werden würden.



Reiter Ausschlüsse

1. Klicken Sie auf die Schaltfläche **Neu anlegen**, um eine neue benutzerdefinierte Ausschlussregel anzulegen. Weitere Einzelheiten finden Sie im Abschnitt Erstellen von benutzerdefinierten Ausschlussregeln.

   Alternativ können Sie jederzeit eine Regel direkt aus dem Vorfallsdiagramm heraus erstellen, indem Sie einen Zielknoten auswählen und ihn über das entsprechende seitliche Detailfenster als Ausschluss hinzufügen. Weitere Einzelheiten finden Sie unter der Funktion Als EDR-Ausschluss hinzufügen.

2. Über die folgenden Schaltflächen können Sie die Anzeige anpassen:

   - Über die Schaltfläche **Spalten ein-/ausblenden** können Sie einzelne Filterspalten hinzufügen oder entfernen.

     Die Seite wird automatisch mit den Karten neu geladen, deren Daten zu den hinzugefügten Spalten passen.

     Über die Schaltfläche **Zurücksetzen** im Klappmenü **Spalten ein-/ausblenden** können Sie die Filter jederzeit zurücksetzen.

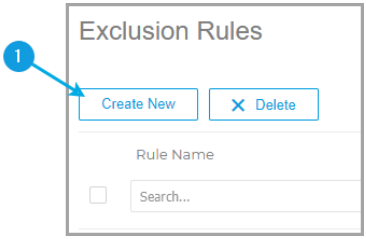
   - Über die Schaltfläche **Filter ein-/ausblenden** können Sie die Filterleiste ein- oder ausblenden.

- Über die Schaltfläche **Neu laden** können Sie die Liste neu laden.

3. Markieren Sie das Sammelkästchen oder die einzelnen Kästchen der Regeln, um sie auszuwählen, und klicken Sie auf **Löschen**, um sie aus der Liste zu entfernen.
4. Klicken Sie auf eine Regel in der Liste, um den Detailbereich aufzuklappen, die Regeldetails anzuzeigen und sie bei Bedarf zu aktualisieren oder zu löschen. Weitere Einzelheiten finden Sie im Detailfenster für Ausschlussregeln.

Erstellen von benutzerdefinierten Ausschlussregeln

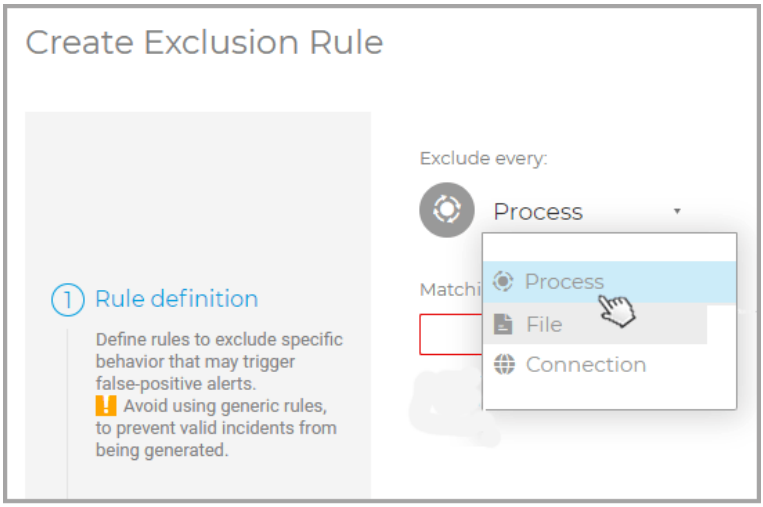
Um eine benutzerdefinierte Ausschlussregel zu erstellen, klicken Sie im Reiter **Ausschlüsse** auf die Schaltfläche **Neu anlegen**.



Erstellung einer neuen Ausschlussregel

Die Seite **Ausschlussregel erstellen** mit dem Abschnitt **Regeldefinition** wird angezeigt. Hier können Sie mit der Bearbeitung der Regel beginnen:

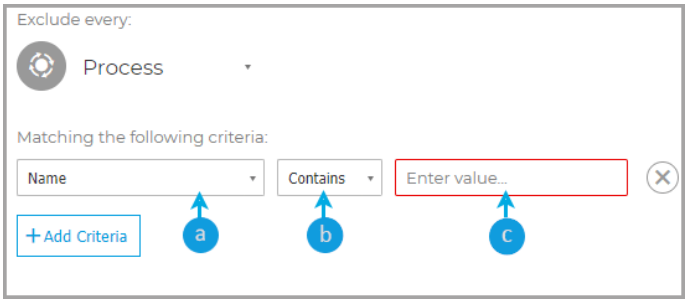
1. Wählen Sie aus, welchen Elementtyp Sie in die Ausschlussregel aufnehmen möchten.



Zur Auswahl stehen:

- Prozess
- Datei
- Verbindung

2. Jeder Elementtyp hat spezifische Übereinstimmungskriterien, die Sie aus dem Dropdown-Menü auswählen können:



a. Wählen Sie eine der verfügbaren Kriterienoptionen aus.

b. Wählen Sie die Art der Beziehung zwischen den Übereinstimmungskriterien und den entsprechenden Wert aus:

- **Ist** - Schließt alle Vorfälle mit Elementen aus, die genau dem im Wertfeld eingegebenen Wert entsprechen.
- **Enthält** - Schließt alle Vorfälle mit Elementen aus, die den im Wertfeld eingegebenen Wert enthalten (z. B. Platzhalter, Dateierweiterungen usw.).

  Wichtig
  Die Verwendung von Platzhaltern bei der Erstellung von Ausschlussregeln erhöht das Risiko, dass sie zu allgemein gehalten werden. So werden konkrete Bedrohungen eher ignoriert und Ihr Unternehmen anfälliger für Angriffe.

- **Ist eines von** - schließt alle Vorfälle mit Elementen aus, die mit einem der im Wertfeld eingegebenen Werte übereinstimmen (der Operator **ODER** wird zwischen den eingegebenen Werten angewendet).

c. Geben Sie den spezifischen Wert für jedes Kriterium ein.

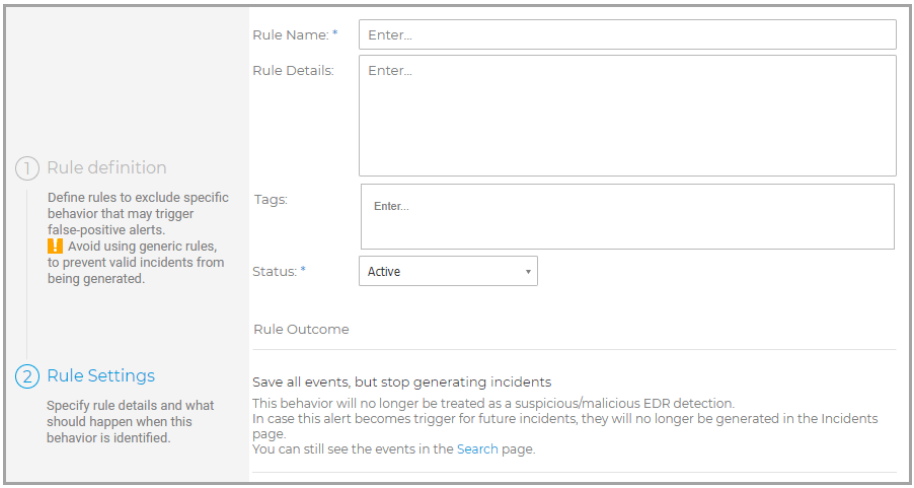
Beachten Sie
Wenn Sie mehrere Werte für ein Kriterium eingeben (bei Verwendung der Bedingung **Ist eine von**), müssen Sie nach jedem Wert **Eingabe** drücken, um die Aktion abzuschließen.

3. Klicken Sie auf **Kriterien hinzufügen**, um der Regel ein neues Kriterium hinzuzufügen.

Beachten Sie
Die Regel schließt die Vorfälle aus, die alle definierten Kriterien enthalten (der Operator **UND** wird zwischen mehreren hinzugefügten Kriterien angewendet).

4. Nachdem alle Kriterien definiert sind, klicken Sie auf **Nächster Schritt**.

   Der Abschnitt **Regeleinstellungen** wird angezeigt, wo Sie die Regeldetails ausfüllen müssen.

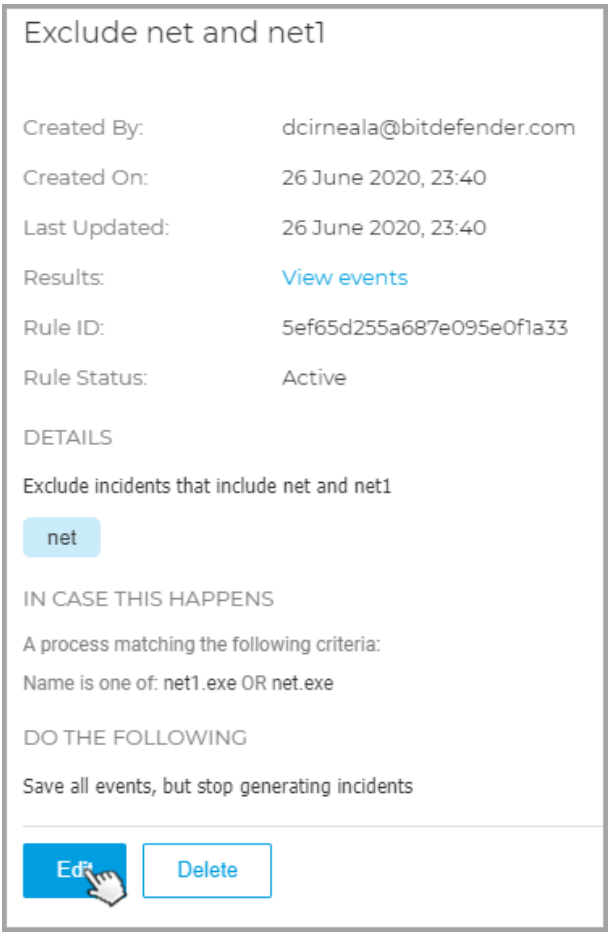


5. Benennen Sie die neue Regel im Feld **Regelname**. Dies ist ein Pflichtfeld.
6. Fügen Sie eine kurze Beschreibung der Regel im Textbereich **Regeldetails** hinzu.
7. Fügen Sie für diese Regel spezifische Tags im Feld **Tag** hinzu, um die Gruppierung und Verwaltung von Regeln zu erleichtern.
8. Legen Sie den Regelstatus über das Dropdown-Menü *Status* auf Aktiv oder Inaktiv fest.
9. Klicken Sie auf **Regel erstellen**, um die Erstellung der benutzerdefinierten Ausschlussregel abzuschließen.

   Sie finden die neue Regel auf der Seite **Ausschlussregeln**.

Detailfenster für Ausschlussregeln

Im Bereich **Regeldetails** finden Sie detaillierte Informationen über die ausgewählte Regel, einschließlich Erstellungsdatum und Ersteller, Datum der letzten Aktualisierung, eindeutige ID und Status sowie einen Link zu einer Liste von Ereignissen, die den Kriterien der Regel entsprechen. Hier finden Sie zudem eine Beschreibung der Regel, die zugehörigen Tags, die enthaltenen Übereinstimmungskriterien und das Ergebnis der Regel.



Bereich Regeldetails

- Klicken Sie auf **Bearbeiten**, um die Seite **Ausschlussregel erstellen** aufzurufen, auf der Sie die Regeldefinition aktualisieren können.
- Klicken Sie auf **Löschen**, um die Ausschlussregel aus der Liste zu entfernen.

10. VERWALTEN VON ENDPUNKTRISIKEN

Die Endpunkt-Risikoanalyse (ERA) dient der Bewertung und Härtung der Sicherheitskonfiguration Ihrer Endpunkte gemäß branchenüblichen Best Practices, um die Angriffsfläche zu reduzieren.

Wichtig
Das Endpoint-Risk-Analytics-Modul steht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Die ERA sammelt und analysiert Daten mithilfe von Risiko-Scan-Aufgaben, die auf bestimmten Geräten in Ihrem Netzwerk ausgeführt werden.

Dazu müssen Sie sich zunächst versichern, dass das ERA-Modul in der Richtlinie, die für die gewünschten Geräte gilt, aktiviert ist:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf die Schaltfläche **Hinzufügen** und nehmen Sie die Einstellungen unter **Allgemein** vor.
3. Markieren Sie in der Liste die Richtlinie **Risiko-Management**.
4. Markieren Sie das Kästchen, um die **Risiko-Management**-Funktionen zu aktivieren. Sie können dann Richtlinien erstellen, die festlegen, wie **Risiko-Scan**-Aufgaben durchgeführt werden.

Beachten Sie
Weitere Informationen zu den Risikoindikatoren in GravityZone finden Sie in diesem Artikel in der Wissensdatenbank.
Weitere Details zu bekannten Anwendungsschwachstellen finden Sie auf dieser Website.

So führen Sie Risiko-Scans durch:

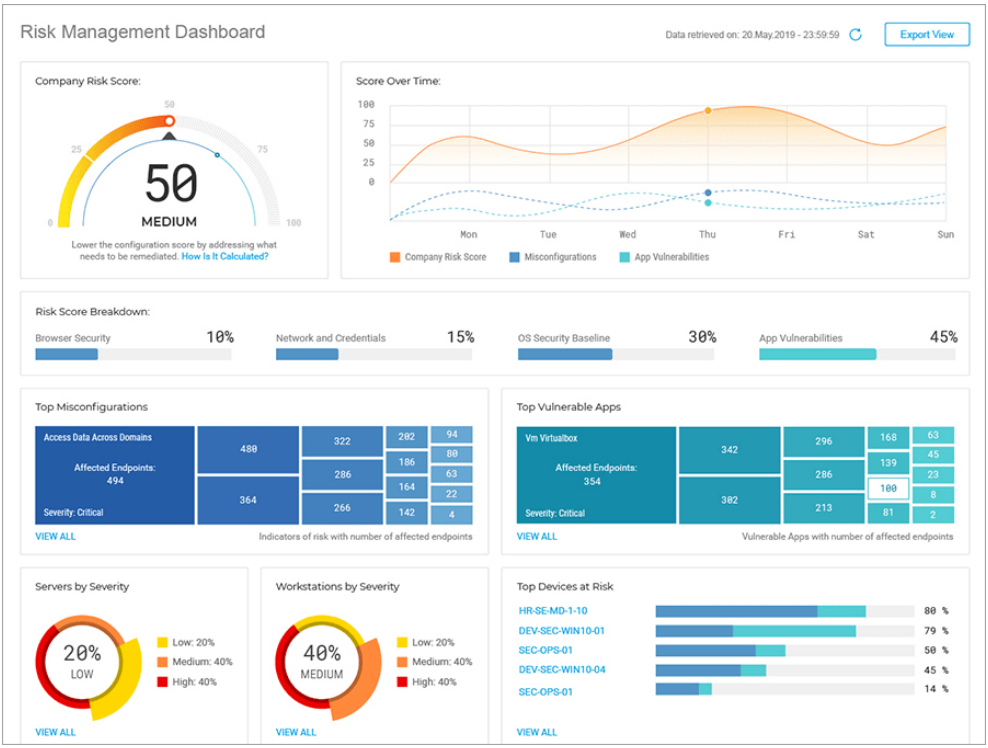
1. Es gibt zwei Möglichkeiten zur Ausführung von Risiko-Scan-Aufgaben auf den Endpunkten:
   a. Bei Bedarf- durch Auswahl der Endpunkte auf der **Netzwerk**-Seite oder durch die Übermittlung einer **Risiko-Scan**-Aufgabe über das Menü **Aufgaben**.
   b. Geplant - durch Konfiguration einer Risiko-Scan-Aufgabe über die Richtlinie, die dann auf den Zielendpunkten automatisch im gewählten Intervall ausgeführt wird.

Nach erfolgreichem Abschluss des Risiko-Scans errechnet GravityZone eine Risikobewertung für jeden Endpunkt..

2. Rufen Sie das **Risiko-Management**-Dashboard auf, um die folgenden Informationen zu erhalten:
   - Die Risikobewertung des Unternehmens und deren Verlauf
   - Risikobewertungen und Statistiken unterteilt in Fehlkonfigurationen, anfällige Apps, menschliche Risiken und betroffene Geräte.
   - Die Beschreibung jedes Risikoindikators und der empfohlenen Bereinigungsaktionen.
3. Auf der Seite Sicherheitsrisiken können Sie die gefundenen Fehlkonfigurationen, Anwendungsschwachstellen und möglicherweise durch Benutzerverhalten hervorgerufene Risiken analysieren und Gegenmaßnahmen ergreifen.

10.1. Das Risiko-Management-Dashboard

Auf der Seite **Risiko-Management** finden Sie einen Überblick mit Informationen zur Netzwerksicherheit und zur Risikobewertung.



Risiko-Management-Dashboard

1. Risikobewertung des Unternehmens
2. Bewertung im Zeitverlauf
3. Häufigste Fehlkonfigurationen
4. Häufigste anfällige Apps
5. Häufigste Risiken durch den Faktor Mensch
6. Server nach Schweregrad
7. Arbeitsplatzrechner nach Schweregrad
8. Gefährdetste Geräte
9. Top-Benutzer nach Sicherheitsverhalten

Die Daten auf dieser Seite sind in mehreren Widgets organisiert:

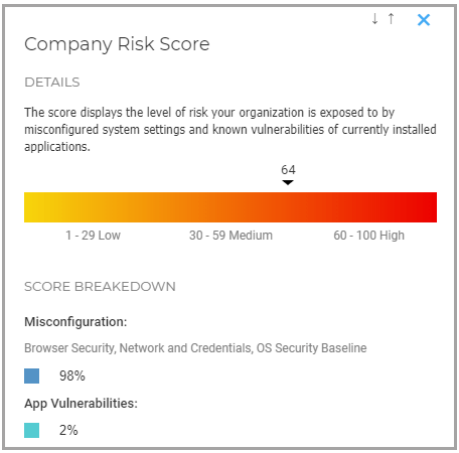
Risikobewertung des Unternehmens

Die Gesamtrisikobewertung zeigt den Grad des Risikos an, dem Ihr Unternehmen durch falsch konfigurierte Systemeinstellungen, bekannte Schwachstellen in den aktuell installierten Anwendungen sowie durch das Verhalten von Benutzern ausgesetzt ist. Diese Bewertung wird durch den Branchenmodifikator (Health Industry Modifier) dynamisch angepasst, der das Risiko durch ausgenutzte Schwachstellen in Apps angibt, die für Ihre Branche charakteristisch sind.

Der Wert ist ein Durchschnitt aus den drei Hauptrisikokategorien **Fehlkonfiguration**, **App-Schwachstellen** und **Risiken durch den Faktor Mensch**.

Widget für die Risikobewertung von Unternehmen

Wenn Sie auf das Widget klicken, wird ein Detailfenster angezeigt, in dem die Berechnung des Gesamtrisikos dargestellt und in Subkategorien unterteilt wird.

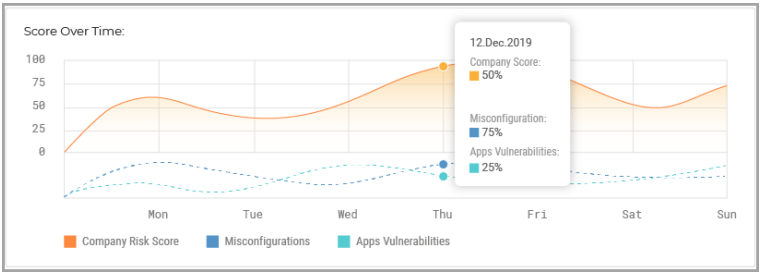


Detailfenster zur Risikobewertung von Unternehmen

Beachten Sie
Die Durchführung eines Risiko-Scans auf einem neuen Gerät verändert die Gesamtbewertung. Die Ergebnisse werden 90 Tage lang oder bis zum nächsten Scan aufbewahrt.

Bewertung im Zeitverlauf

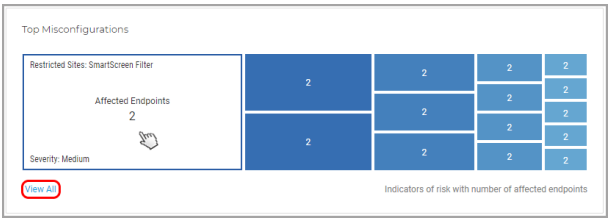
Dieses Widget ist ein Histogramm, in dem die die zeitliche Entwicklung des Risikos anhand der Anzahl der betroffenen Geräte dargestellt wird. Diese Zahl wird durch wöchentliche Risiko-Scans ermittelt. Die Histogrammdaten stellen die Anzahl der von Risikoindikatoren betroffenen Geräten der vergangenen 7 Tage bis 12 Uhr (Serverzeit) des aktuellen Tages dar.



Widget zur Risikobewertung im zeitlichen Verlauf

Häufigste Fehlkonfigurationen

In diesem Widget werden die 15 Risikoindikatoren dargestellt, die beim Scan der Geräte am häufigsten eine Risikowarnmeldung ausgelöst haben. Sortiert sind sie nach der Anzahl der betroffenen Geräte. Jede Karte stellt einen Indikator dar, der eine Risikowarnmeldung für mindestens einen Endpunkt ausgelöst hat.



Widget zu den häufigsten Fehlkonfigurationen

Auf jeder Karte sind die folgenden Elemente enthalten:

- Der Name des Indikators.
- Die Anzahl der Geräte, die für diesen Indikator als anfällig erkannt wurden.
- Der Schweregrad der Fehlkonfiguration.

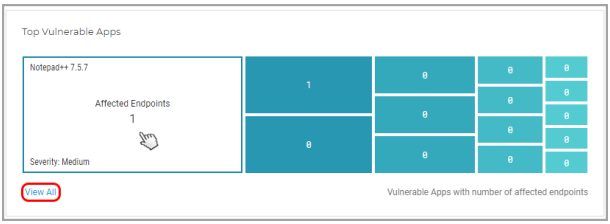
Wenn Sie auf das jeweilige Indikator-Widget klicken, öffnet sich der ausgewählte Risikoindikator im Reiter Fehlkonfigurationen auf der Seite **Sicherheitsrisiken**. Hier können Sie geeignete Maßnahmen ergreifen, um dieses Risiko zu mindern.

Wenn Sie auf **Alle anzeigen** klicken, werden alle gefundenen Fehlkonfigurationen im Reiter Fehlkonfigurationen der Seite **Sicherheitsrisiken** angezeigt.

Beachten Sie
Weitere Informationen zum Thema Fehlkonfigurationen finden Sie in diesem Artikel der Wissensdatenbank.

Häufigste anfällige Apps

In diesem Widget werden die 15 bekannten App-Schwachstellen dargestellt, die beim Scan der Geräte am häufigsten eine Risikowarnmeldung ausgelöst haben. Sortiert sind sie nach der Anzahl der betroffenen Geräte. Jede Karte stellt eine anfällig Anwendung dar, die eine Risikowarnmeldung für mindestens einen Endpunkt ausgelöst hat.



Widget der häufigsten anfälligen Apps

Auf jeder Karte sind die folgenden Elemente enthalten:

- Der Name der Anwendung
- Die Anzahl der Geräte, die durch diese Anwendung anfällig geworden sind
- Der Schweregrad der anfälligen Anwendung

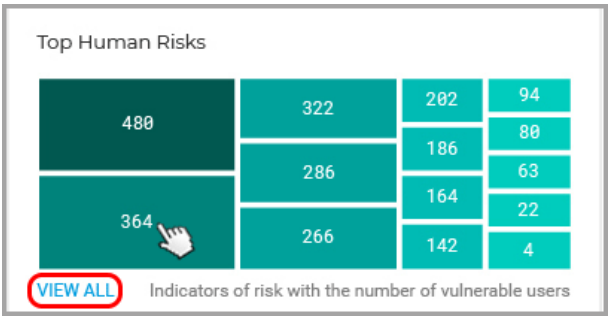
Wenn Sie auf das jeweilige App-Widget klicken, öffnet sich die ausgewählte Schwachstelle im Reiter Anwendungsschwachstellen auf der Seite **Sicherheitsrisiken**. Hier können Sie geeignete Maßnahmen zur Minderung dieses Risikos ergreifen.

Wenn Sie auf **Alle anzeigen** klicken, werden alle gefundenen App-Schwachstellen im Reiter App-Schwachstellen der Seite **Sicherheitsrisiken** angezeigt.

Beachten Sie
Weitere Details zu bekannten Anwendungsschwachstellen finden Sie auf dieser Website.

Häufigste Risiken durch den Faktor Mensch

Dieses Widget zeigt die 15 häufigsten Ergebnisse für potenzielle Risiken, die durch unbeabsichtigtes oder fahrlässiges Verhalten der in Ihrem Netzwerk aktiven Benutzern verursacht werden, geordnet nach der Anzahl der gefährdeten Benutzer. Jede Karte stellt ein menschliches Risiko dar, das von mindestens einem Benutzer verursacht wird.



Widget Häufigste Risiken durch den Faktor Mensch

Auf jeder Karte sind die folgenden Elemente enthalten:

- Name des menschlichen Risikos.
- Die Anzahl der Benutzer, deren fahrlässiges oder unbeabsichtigtes Verhalten Ihr Unternehmen gefährden könnte.
- Der Schweregrad des menschlichen Risikos.

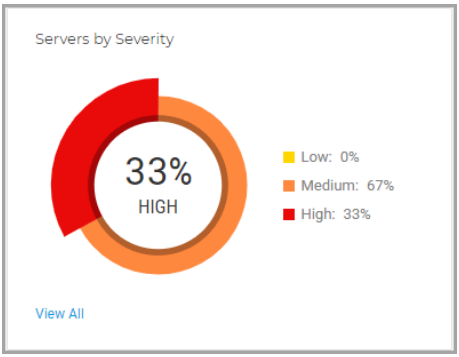
Wenn Sie auf das jeweilige Widget für die menschlichen Risiken klicken, öffnet sich das ausgewählte Risiko im Reiter Risiken durch den Faktor Mensch auf der Seite **Sicherheitsrisiken**. Hier können Sie es im Detail betrachten und analysieren.

Wenn Sie auf **Alle anzeigen** klicken, sehen Sie im Reiter Risiken durch den Faktor Mensch der Seite **Sicherheitsrisiken** die gesamte Liste aller entdeckten menschlichen Risiken, die durch Benutzerverhalten ausgelöst wurden.

Beachten Sie
Diese neue ERA-Funktion ist als Vorschauversion verfügbar, so dass Sie nur die vom Menschen ausgehenden Risiken anzeigen und diese ignorieren können, wenn sie für Ihre Umgebung nicht relevant sind. Die Funktionalität wird in naher Zukunft weiter ausgebaut.

Server nach Schweregrad

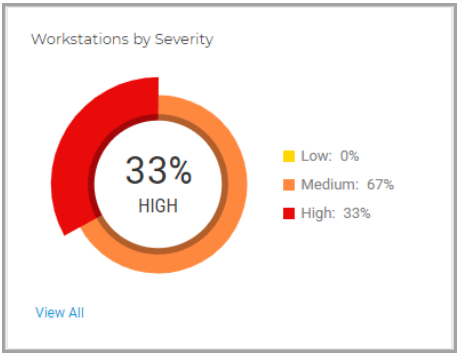
In diesem Widget wird der Schweregrad der Risiken dargestellt, denen die Server in Ihrer Umgebung ausgesetzt sind. Der Anteil der gefundenen Fehlkonfigurationen und App-Schwachstellen ist dort in Prozent angegeben.



Widget für Server nach Schweregrad

Arbeitsplatzrechner nach Schweregrad

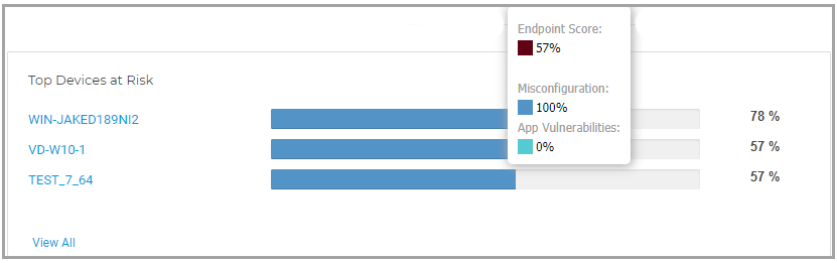
In diesem Widget ist der Schweregrad der Risiken dargestellt, denen die Arbeitsplatzrechner in Ihrer Umgebung ausgesetzt sind. Der Anteil der gefundenen Fehlkonfigurationen und App-Schwachstellen ist dort in Prozent angegeben.



Widget für die Arbeitsplatzrechner nach Schweregrad

Gefährdetste Geräte

In diesem Widget werden die anfälligsten Server und Arbeitsplatzrechner Ihrer Umgebung angezeigt. Gemessen wird dies an der Gesamtrisikobewertung nach den Scans auf Fehlkonfigurationen und Schwachstellen.

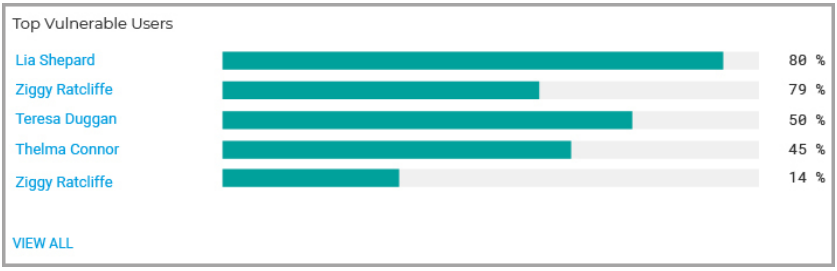


Widget für die Gefährdetsten Geräte

Wenn Sie auf **Alle anzeigen** klicken, sehen Sie im Reiter Geräte auf der Seite **Sicherheitsrisiken** die gesamte Liste der Geräte, die potentiellen Bedrohungen ausgesetzt sind.

Häufigste anfällige Benutzer

Dieses Widget zeigt Ihnen die am stärksten gefährdeten Benutzer in Ihrer Umgebung, entsprechend der Gesamtbewertung, die nach der Analyse ihres Verhaltens und ihrer Aktivität berechnet wurde.

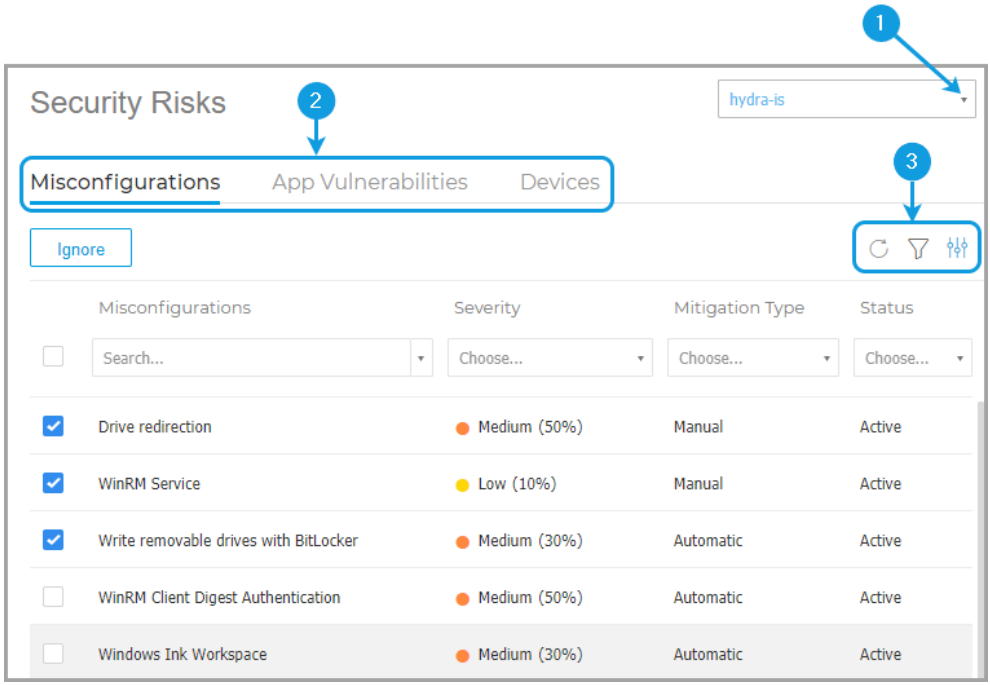


Widget Häufigste anfällige Benutzer

Wenn Sie auf **Alle anzeigen** klicken, sehen Sie im Reiter Benutzer auf der Seite **Sicherheitsrisiken** die gesamte Liste der Benutzer, die Ihr Unternehmen durch ihr Verhalten einem möglichen Sicherheitsrisiko ausgesetzt haben.

10.2. Sicherheitsrisiken

Auf dieser Seite werden alle Risiken, betroffenen Geräte und gefährdeten Benutzer angezeigt, die in Ihrer Umgebung über **Risiko-Scan**-Aufgabe gefunden wurden.



Die Sicherheitsrisikenseite

Die Risikoindikatoren werden in einem Raster angezeigt, das durch zahlreiche Filter an die momentanen Bedürfnisse angepasst werden kann:

1. Wählen Sie ein Unternehmen, das Sie verwalten und dessen Risiken Sie analysieren möchten.
2. Wählen Sie eine Kategorie, die Sie untersuchen möchten:
   - Fehlkonfigurationen
   - App-Schwachstellen
   - Risiken durch den Faktor Mensch
   - Geräte
   - Benutzer

3. Über die folgenden Schaltflächen können Sie die Anzeige anpassen:
   - Über die Schaltfläche **Spalten ein-/ausblenden** können Sie einzelne Filterspalten hinzufügen oder entfernen.

     Die Seite wird automatisch mit den Karten der Risikoindikatoren neu geladen, deren Daten zu den hinzugefügten Filterspalten passen.

     Über die Schaltfläche **Zurücksetzen** im Klappmenü **Spalten ein-/ausblenden** können Sie die Filter jederzeit zurücksetzen.
   - Über die Schaltfläche **Filter ein-/ausblenden** können Sie die Filterleiste ein- oder ausblenden.
   - Über die Schaltfläche **Neu laden** können Sie die Liste neu laden.

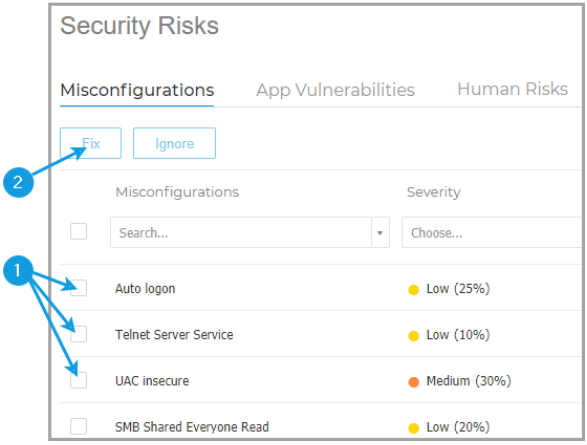
Jede Risikoindikator wird als Rich Card dargestellt, auf der je nach den eingestellten Filtern die relevanten Informationen zu diesem Risikoindikator angezeigt werden.

Fehlkonfigurationen

Im Reiter **Fehlkonfigurationen** werden standardmäßig alle GravityZone-Risikoindikatoren angezeigt. Hier werden Details zum Schweregrad, zur Anzahl der betroffenen Geräte, zum Fehlkonfigurationstyp, zur Art der Abhilfemaßnahme (manuell oder automatisch) und zum Status (aktiv oder ignoriert) angezeigt.

Gehen Sie folgendermaßen vor, um mehrere Fehlkonfigurationen gleichzeitig zu beheben:

1. Markieren Sie das Sammelkästchen oder die einzelnen Kästchen der gewünschten Risikoindikatoren.



Behebung mehrerer Risiken im Reiter Fehlkonfigurationen

2. Klicken Sie auf **Risiken beheben**.

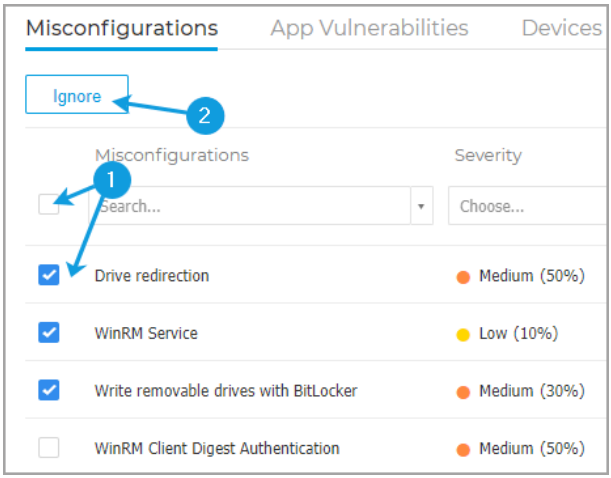
   In einem neuen Fenster müssen Sie die Aktion bestätigen (oder abbrechen).

3. Hierdurch wird eine neue Aufgabe erstellt, mit der die empfohlene Änderung auf allen betroffenen Geräten vorgenommen wird.

> **Beachten Sie**
> Auf der Seite **Netzwerk** > **Aufgaben** wird der Fortschritt der Aufgabe dargestellt. Wenn das Risiko nur manuell behoben werden kann, müssen Sie direkt auf die betroffenen Geräte zugreifen und die entsprechende Änderung selbst vornehmen.

Gehen Sie folgendermaßen vor, um den Status von Fehlkonfigurationen zu ändern:

1. Markieren Sie das Sammelkästchen oder die einzelnen Kästchen der gewünschten Risikoindikatoren.



Änderung des Status mehrerer Risiken im Reiter Fehlkonfigurationen

2. Klicken Sie auf die Schaltfläche **Risiken ignorieren/wiederherstellen** um den Status von **Aktiv** auf **Ignoriert** (oder umgekehrt) zu setzen.

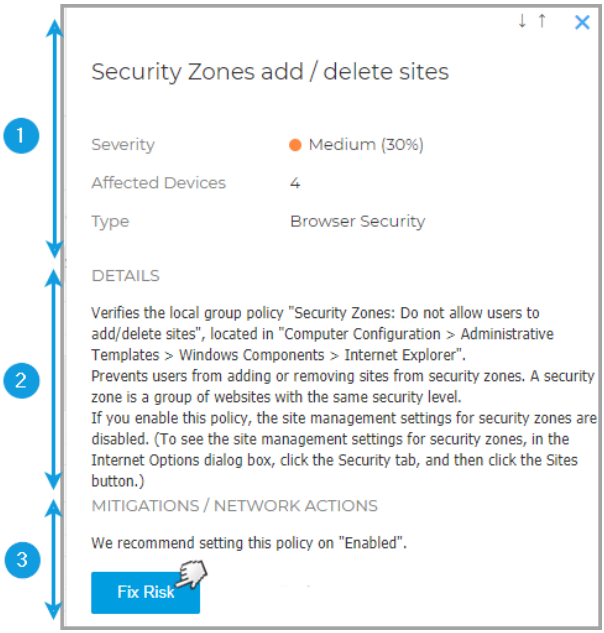
> **Beachten Sie**
> Die Aktion **Risiken ignorieren** wird auf alle ausgewählten Geräte angewendet und wirkt sich beim nächsten Risiko-Scan auf die Gesamtrisikobewertung des Unternehmen aus. Wir empfehlen dringend, die Auswirkungen auf die Sicherheit Ihres Unternehmens zu bedenken, wenn Sie Risikoindikatoren ignorieren.

Über die folgenden Filteroptionen können Sie die auf den Karten angezeigten Informationen zu Fehlkonfigurationen anpassen:

Filterungsoptionen	Details
Fehlkonfiguration	Diese Spalte enthält ein durchsuchbares Klappmenü, über das Sie die Liste der Indikatoren nach Name durchsuchen können.
Schweregrad	In dieser Spalte können Sie die Risikoindikatoren nach Schweregrad filtern. Hier können Sie Gering, Mittel oder Hoch wählen.

Filterungsoptionen	Details
Betroffene Geräte	In dieser Spalte ist die Anzahl der Server und Arbeitsplatzrechner angegeben, die durch einen bestimmten Risikoindikator evtl. gefährdet sind.
Typ	In dieser Spalte können Sie die Risikoindikatoren nach Typ filtern: • Browser-Sicherheit • Netzwerk und Zugangsdaten • Betriebssystemsicherheit
Art der Abhilfemaßnahme	In dieser Spalte können Sie die Risikoindikatoren nach der Art der Abhilfemaßnahme (manuell oder automatisch) filtern.
Status	In dieser Spalte können Sie die Risikoindikatoren nach ihrem Status (aktiv oder ignoriert) filtern.

Klicken Sie auf die Fehlkonfiguration, die Sie analysieren möchten, um den dazugehörigen Seitenbereich zu öffnen.



Detailfenster für Fehlkonfigurationen

In jedem Detailfenster sind die folgenden Elemente enthalten:

1. Ein Infobereich mit dem Namen des Risikoindikators, seinem Schweregrad, der Anzahl der betroffenen Geräte und dem Typ.
2. Ein **Details**-Bereich, in dem die Einstellung und ihre Konfigurationsoptionen beschrieben werden.
3. Ein Bereich **Abhilfemaßnahmen / Netzwerkaktionen** mit Empfehlungen zur Verringerung des Risikos für die betroffenen Geräte und mögliche Aktionen.
   a. Wenn Sie auf **Risiko beheben** klicken, wird die Konfiguration entsprechend der Empfehlung angepasst.

      In einem neuen Fenster müssen Sie die Aktion bestätigen (oder abbrechen).

   b. Hierdurch wird eine neue Aufgabe erstellt, mit der die empfohlene Änderung auf allen betroffenen Geräten vorgenommen wird.

> **Beachten Sie**
> Auf der Seite **Netzwerk** > **Aufgaben** wird der Fortschritt der Aufgabe dargestellt. Wenn das Risiko nur manuell behoben werden kann, müssen Sie direkt auf die betroffenen Geräte zugreifen und die entsprechende Änderung selbst vornehmen.

c. Über die Schaltfläche **Risiko ignorieren** ändern Sie den Status des ausgewählten Risikos von **Aktiv** auf **Ignoriert**.

> **Beachten Sie**
> Sie können es jederzeit wieder in den aktiven Zustand zurückversetzen, indem Sie auf die Schaltfläche **Risiko wiederherstellen** klicken.

d. Mit einem Klick auf **Geräte anzeigen** wird der Reiter Geräte geöffnet, in dem alle Geräte angezeigt werden, die aktuell von diesem Risikoindikator betroffen sind.

App-Schwachstellen

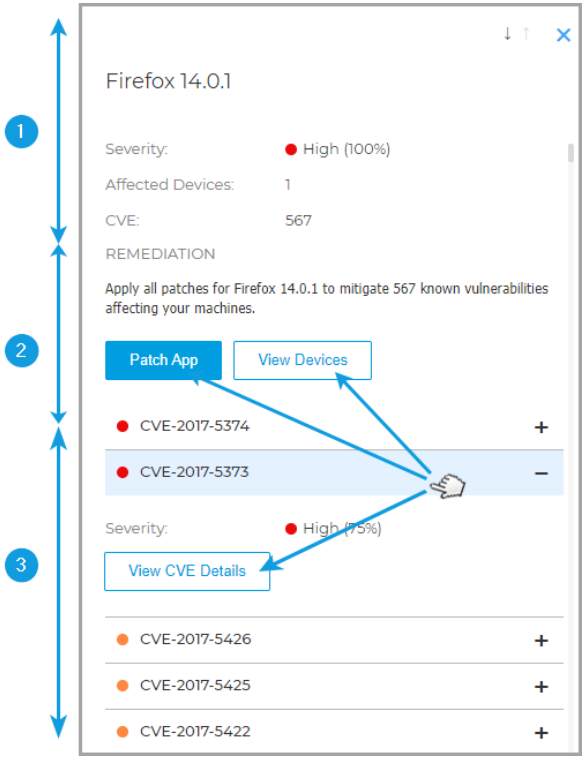
Im Reiter **App-Schwachstellen** werden alle Anwendungen angezeigt, die bei einem Risiko-Scan auf Geräten in Ihrer Umgebung gefunden wurden. Dort sind detaillierte Informationen zum Schweregrad, zur Anzahl an bekannten CVEs pro Anwendung und zur Anzahl der betroffenen Geräte aufgeführt.

Über die folgenden Filteroptionen können Sie die auf den Karten angezeigten Informationen zu anfälligen Anwendungen anpassen:

Filterungsoptionen	Details
Anwendungen	Diese Spalte enthält ein durchsuchbares Klappmenü, über das Sie die Liste der anfälligen Anwendungen nach Name filtern können.
Schweregrad	In dieser Spalte können Sie die Liste der anfälligen Anwendungen nach Schweregrad filtern. Hier können Sie Gering, Mittel oder Hoch wählen.
CVE	In dieser Spalte wird die Anzahl der CVEs für jede in ihrer Umgebung installierte Anwendung angezeigt.

Filterungsoptionen	Details
Betroffene Geräte	In dieser Spalte ist die Anzahl der Server und Arbeitsplatzrechner angegeben, die durch einen bestimmten Risikoindikator evtl. gefährdet sind.

Wenn Sie auf eine der aufgeführten Anwendungen klicken, werden mehr Details dazu angezeigt.



Detailfenster für anfällige Anwendungen

In jedem Detailfenster sind die folgenden Elemente enthalten:

1. Ein Infobereich mit dem Namen der Anwendung, dem Schweregrad, der Anzahl der betroffenen Geräte und der Anzahl der Exploits, die Ihre Umgebung manipuliert haben.
2. Der Bereich **Bereinigung** mit Abhilfemaßnahmen und einer Liste der gefundenen CVEs:
   a. Wenn Sie auf **Anwendung patchen** klicken, können Sie verfügbare Patches für die anfällige Anwendung installieren.

      Wichtig
      Die Aktion **Anwendung patchen** funktioniert nur für Geräte, auf denen das Modul Patch-Verwaltung installiert ist.

      In einem neuen Fenster müssen Sie die Aktion bestätigen (oder abbrechen).

   b. Hierdurch wird eine neue Aufgabe erstellt, mit der die Patches für anfällige Anwendungen auf allen betroffenen Geräten installiert werden.

      Beachten Sie
      Auf der Seite **Netzwerk** > **Aufgaben** wird der Fortschritt der Aufgabe dargestellt.

   c. Über die Schaltfläche **App ignorieren** ändern Sie den Status der ausgewählten App von **Aktiv** auf **Ignoriert**.

      Beachten Sie
      Sie können sie jederzeit wieder in den aktiven Zustand zurückversetzen, indem Sie auf die Schaltfläche **App wiederherstellen** klicken.

3. Wenn Sie die Anzeige einer aufgeführten CVE erweitern und dann auf **CVE-Details anzeigen** klicken, können Sie weitere Details zu dieser CVE aus der Datenbank abrufen.

Risiken durch den Faktor Mensch

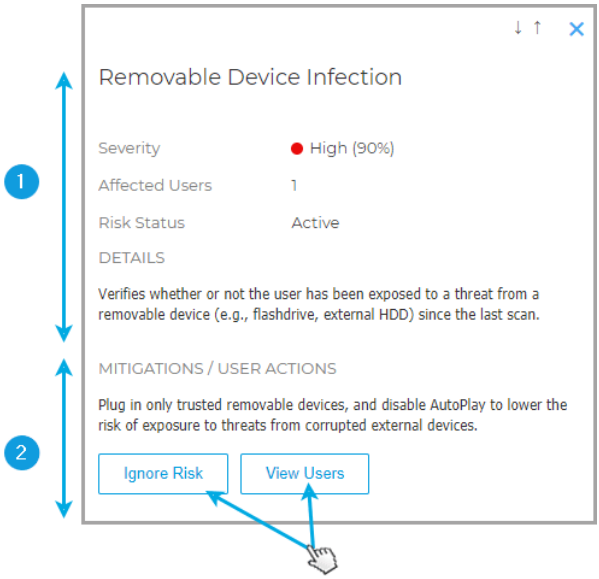
Im Reiter **Risiken durch den Faktor Mensch** finden Sie alle Risiken, die durch fahrlässige oder unbeabsichtigte Aktionen aktiver Benutzer oder fehlende Maßnahmen zur ordnungsgemäßen Sicherung ihrer Arbeitssitzungen in Ihrem Netzwerk verursacht werden. Hier finden Sie detaillierte Informationen zum Schweregrad, die Anzahl der gefährdeten Benutzer, den Risikostatus und -typ.

Beachten Sie
Unter Datenerhebung zu menschlichen Risiken finden Sie weitere Einzelheiten dazu, wie wir Benutzerdaten verarbeiten.

Über die folgenden Filteroptionen können Sie die auf den Karten angezeigten Informationen zu den Risiken durch den Faktor Mensch anpassen:

Filterungsoptionen	Details
Risiken durch den Faktor Mensch	Diese Spalte enthält ein durchsuchbares Klappmenü, über das Sie die Liste der menschlichen Risiken nach Name filtern können.
Schweregrad	Über diese Spalte können Sie die Liste der menschlichen Risiken nach ihrem Schweregrad filtern. Hier können Sie Gering, Mittel oder Hoch wählen.
Anfällige Benutzer	Diese Spalte zeigt die Anzahl der Benutzer von denen menschliche Risiken ausgehen.
Art der Abhilfemaßnahme	In dieser Spalte können Sie die Liste der Risiken nach der Art der Abhilfemaßnahme (manuell oder automatisch) filtern.
Status	In dieser Spalte können Sie die Liste der Risiken nach ihrem Status (aktiv oder ignoriert) filtern.

Klicken Sie auf das menschliche Risiko, das Sie analysieren möchten, um den dazugehörigen Seitenbereich zu öffnen.



Detailbereich für menschliche Risiken

In jedem Detailfenster sind die folgenden Elemente enthalten:

1. Ein Infobereich mit dem Namen des Risikos, dem Schweregrad, den gefährdeten Benutzern, dem Risikostatus und einer detaillierten Beschreibung des Risikos.
2. Einen Bereich **Abhilfemaßnahmen/Benutzeraktionen** mit Abhilfemaßnahmen:
   a. Über die Schaltfläche **Risiko ignorieren** ändern Sie den Status des ausgewählten Risikos von **Aktiv** auf **Ignoriert**.

      Beachten Sie
      Sie können es jederzeit wieder in den aktiven Zustand zurückversetzen, indem Sie auf die Schaltfläche **Risiko wiederherstellen** klicken.

   b. Über **Benutzer anzeigen** rufen Sie den Reiter Benutzer auf. Hier werden alle Benutzer angezeigt, die dieses Risiko ausgelöst haben, während sie in Ihrem Netzwerk aktiv waren.

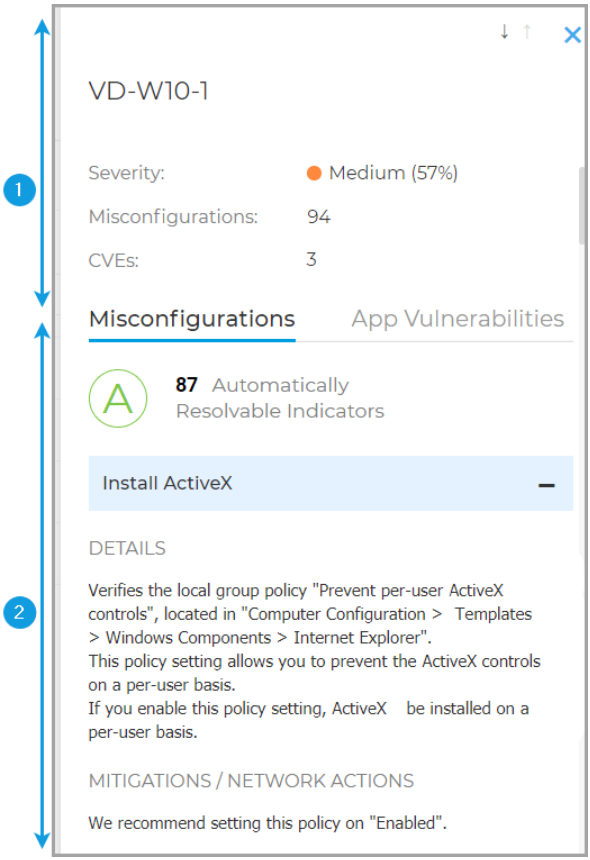
Geräte

Im Reiter **Geräte** werden alle gescannten Server und Arbeitsplatzrechner angezeigt, die Sie verwalten. Hier werden Details zum Namen, Schweregrad, Gerätetyp und zur Anzahl der Risiken angezeigt, die das jeweilige Gerät betreffen.

Über die folgenden Filteroptionen können Sie die auf den Karten angezeigten Informationen zu den Geräten anpassen:

Filterungsoptionen	Details
Gerät	Diese Spalte enthält ein durchsuchbares Klappmenü, über das Sie die Liste der betroffenen Server und Arbeitsplatzrechner nach Name filtern können.
Schweregrad	In dieser Spalte können Sie die Liste der Geräte nach dem Schweregrad filtern, der für die jeweiligen Geräte gilt. Hier können Sie Gering, Mittel oder Hoch wählen.
Fehlkonfigurationen	In dieser Spalte wird die Anzahl der Fehlkonfigurationen angezeigt, die auf den Geräten gefunden wurden.
CVEs	In dieser Spalte wird die Anzahl der CVEs angezeigt, die auf den Geräten gefunden wurden.
Gerätetyp	In dieser Spalte können Sie die Liste nach Gerätetyp filtern. Sie können entweder Server oder Arbeitsplatzrechner auswählen.

Wenn Sie auf ein Gerät klicken, werden weitere Details zu diesem Gerät angezeigt.



Detailfenster für Geräte

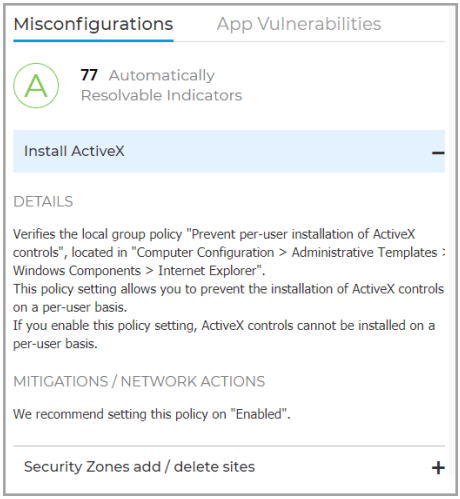
In jedem Detailfenster sind die folgenden Elemente enthalten:

1. Ein Infobereich mit dem Namen des Geräts, dem Schweregrad, der Anzahl der Fehlkonfigurationen und der Anzahl der CVEs auf diesem Gerät.

   Über die Schaltfläche **Endpunkt ignorieren** ändern Sie den Status des ausgewählten Geräts von **Aktiv** auf **Ignoriert**.

   Beachten Sie
   Sie können ihn jederzeit wieder in den aktiven Zustand zurückversetzen, indem Sie auf die Schaltfläche **Endpunkt wiederherstellen** klicken.

2. Im Risikobereich werden alle auf dem Gerät gefundenen Fehlkonfigurationen und anfälligen Anwendungen in zwei Reitern angezeigt.
   - Im Reiter **Fehlkonfigurationen** werden alle auf dem Gerät gefundenen Fehlkonfigurationen angezeigt. Sie sind aufgeteilt in solche, die automatisch behoben werden können, und solche, die manuell behoben werden müssen.



   a. Klicken Sie auf **Alle Risiken beheben**, um alle falsch konfigurierten Einstellungen und Richtlinien, die dieses Gerät betreffen, zu korrigieren.

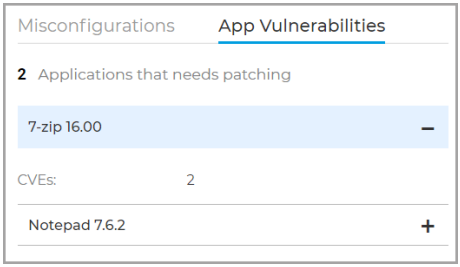
      In einem neuen Fenster müssen Sie die Aktion bestätigen (oder abbrechen).

   b. Hierdurch wird eine neue Aufgabe erstellt, mit der die empfohlene Änderung auf dem betroffenen Gerät vorgenommen wird.

      Beachten Sie
      Auf der Seite **Netzwerk** > **Aufgaben** wird der Fortschritt der Aufgabe dargestellt.
      Für Risikoindikatoren, die nur manuell behoben werden können, müssen Sie direkt auf das betroffene Gerät zugreifen und die empfohlene Konfiguration selbst vornehmen.

> **Beachten Sie**
> Alternativ können Sie auch jede Fehlkonfiguration, die das aktuelle Gerät betrifft, einzeln untersuchen und nacheinander mit der Schaltfläche **Risiko beheben** beheben.

- Im Reiter **App-Schwachstellen** werden alle anfälligen Anwendungen angezeigt, die auf dem Gerät gefunden wurden, sowie die Anzahl an CVEs, die jede Anwendung betreffen.



a. Klicken Sie auf **Alle Apps patchen**, um verfügbare Patches für alle anfälligen Anwendungen anzuwenden, die das ausgewählte Gerät Bedrohungen aussetzen.

> **Wichtig**
> Die Funktion **Alle Apps patchen** funktioniert nur auf gescannten Geräten, auf denen das Modul Patch-Verwaltung installiert ist.

In einem neuen Fenster müssen Sie die Aktion bestätigen (oder abbrechen).

b. Hierdurch wird eine neue Aufgabe erstellt, mit der die Patches für anfällige Anwendungen auf dem betroffenen Gerät installiert werden.

> **Beachten Sie**
> Auf der Seite **Netzwerk** > **Aufgaben** wird der Fortschritt der Aufgabe dargestellt.

Beachten Sie
Alternativ können Sie auch jede anfällige App, die das aktuelle Gerät betrifft, einzeln untersuchen und nacheinander mit der Schaltfläche **App patchen** patchen.

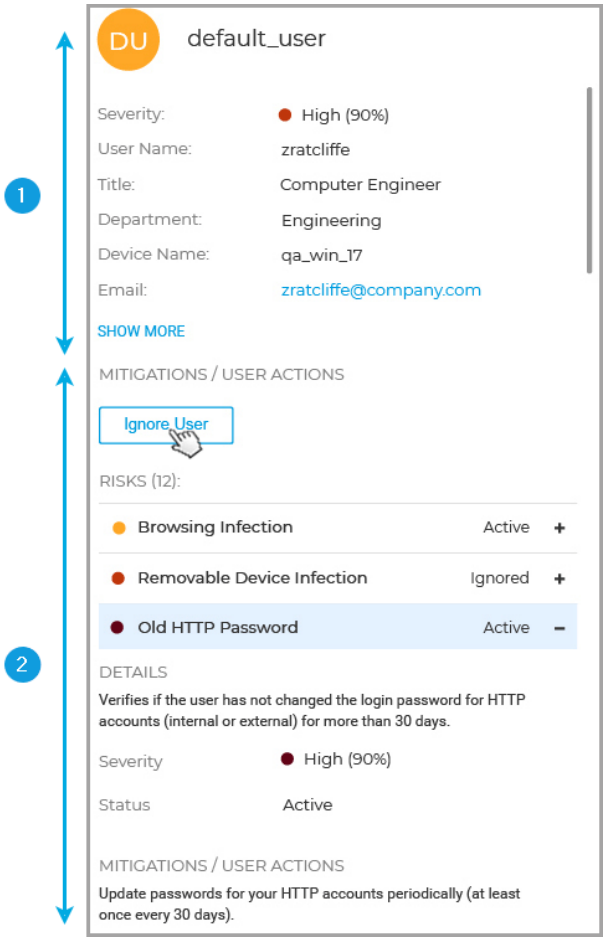
Benutzer

Der Reiter **Benutzer** zeigt alle Benutzer an, die, absichtlich oder unabsichtlich, Ihre Umgebung Bedrohungen aussetzen. Hier finden Sie Informationen wie den Benutzernamen, den Grad der Gesamtrisikoschwere für diesen Benutzer, den Titel und die Abteilung des Benutzers, die Anzahl der Risiken, denen er ausgesetzt ist, und seinen Status in der Berechnung des Gesamtrisikos des Unternehmens.

Über die folgenden Filteroptionen können Sie die auf den Karten angezeigten Informationen zu den Geräten anpassen:

Filterungsoptionen	Details
Benutzer	Diese Spalte enthält ein durchsuchbares Feld, über das Sie die Liste der gefährdeten Benutzer nach Namen filtern können.
Schweregrad	Über diese Spalte können Sie die Liste der gefährdeten Benutzer nach Schweregrad filtern. Hier können Sie Gering, Mittel oder Hoch wählen.
Anzahl an Risiken	Diese Spalte zeigt die Anzahl der menschlichen Risiken, die von den einzelnen Benutzern ausgehen.
Titel	Über diese Spalte können Sie die Liste der Benutzer nach ihrem Titel im Unternehmen filtern.
Abteilung	Über diese Spalte können Sie die Liste der Benutzer nach Abteilung im Unternehmen filtern.
Status	Über diese Spalte können Sie die Liste der Benutzer nach ihrem Status filtern, Aktiv oder Ignoriert.

Klicken Sie auf den Benutzer, den Sie untersuchen möchten, um den dazugehörigen Seitenbereich zu öffnen.



Detailbereich für Benutzer

In jedem Detailfenster sind die folgenden Elemente enthalten:

1. Ein Infobereich mit dem Benutzernamen, Titel und Abteilung, Kontaktinformationen, Schweregrad und Status.
2. Einen Bereich **Abhilfemaßnahmen/Benutzeraktionen** mit Abhilfemaßnahmen:
   a. Über die Schaltfläche **Benutzer ignorieren** ändern Sie den Status des ausgewählten Benutzers von **Aktiv** auf **Ignoriert**.

Beachten Sie
Sie können ihn jederzeit wieder in den aktiven Zustand zurückversetzen, indem Sie auf die Schaltfläche **Benutzer wiederherstellen** klicken.

11. 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).

11.1. Berichtstypen

Für jeden Endpunkttyp stehen eine Reihe von Berichtstypen zur Verfügung:

- Berichte zu Computern und virtuellen Maschinen
- Exchange-Berichte

11.1.1. Berichte zu Computern und virtuellen Maschinen

Im Folgenden werden die verschiedenen Berichttypen 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, Erweiterter Exploit-Schutz und ATC/IDS. 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 Sichrheitsmodule bequem anweisen, die Ausführung der ausgewählten Anwendung auf dem Zielendpunkt zuzulassen:

Klicken Sie auf die Schaltfläche **Ausnahme hinzufügen**, um Ausnahmen in den folgenden Modulen festzulegen: Malware-Schutz, ATC, Inhaltssteuerung und Firewall. Es erscheint ein Bestätigungsfenster mit Informationen zu der neuen Regel, welche die bestehende Richtlinie für diesen spezifischen Endpunkt modifiziert.

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 Zielendpunkt 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.
- Unternehmensname.

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.

Monatslizenznutzung

Wenn Sie auf die Zahlen in den Spalten klicken, werden Details zu den verschiedenen Modulen und Add-ons angezeigt. Sie können den Inhalt des Berichts ganz einfach anpassen, indem Sie auf die Schaltfläche **Spalten ein-/ausblenden** klicken.

Monatslizenznutzung für Email Security

In diesem Bericht sind Informationen zur Nutzung der Monatslizenzen für den Dienst cloud_email_sec] zusammengefasst. In jedem Bericht sind sämtliche Nutzungsinformationen bis zum Ende des vergangenen Tages enthalten. Sagen wir, Sie erstellen an einem Montag um 12 Uhr mittags einen Bericht und stellen den Zeitraum auf **Dieser Monat** ein. Der erstellte Bericht enthält dann sämtliche Lizenznutzungsinformationen bis einschl. Sonntag 23:59 Uhr.

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
- Nutzername
- 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 Zielendpunkte. 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 eingestuften 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 Dateiendungen für die manuelle Übermittlung“ (S. 486).
- 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
- 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.

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 Endpunkt 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.

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.

11.1.2. 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.

Monatslizenznutzung für Exchange

Liefert Ihnen detaillierte Informationen zur Security for Exchange-Lizenznutzung für Ihr Unternehmen über einen bestimmten Zeitraum.

Die Tabelle unter dem Diagramm enthält Informationen wie den Namen des Unternehmens, Lizenzschlüssel, Monat und Anzahl der geschützten Postfächer für Ihr Unternehmen.

Ein Klick auf die Lizenznutzungszahl öffnet ein neues Fenster, in dem detaillierte Informationen zur Nutzung aufgeführt sind, zum Beispiel für Ihr Unternehmen lizenzierte Domains und zugehörige Postfächer.

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.

11.2. Berichte erstellen

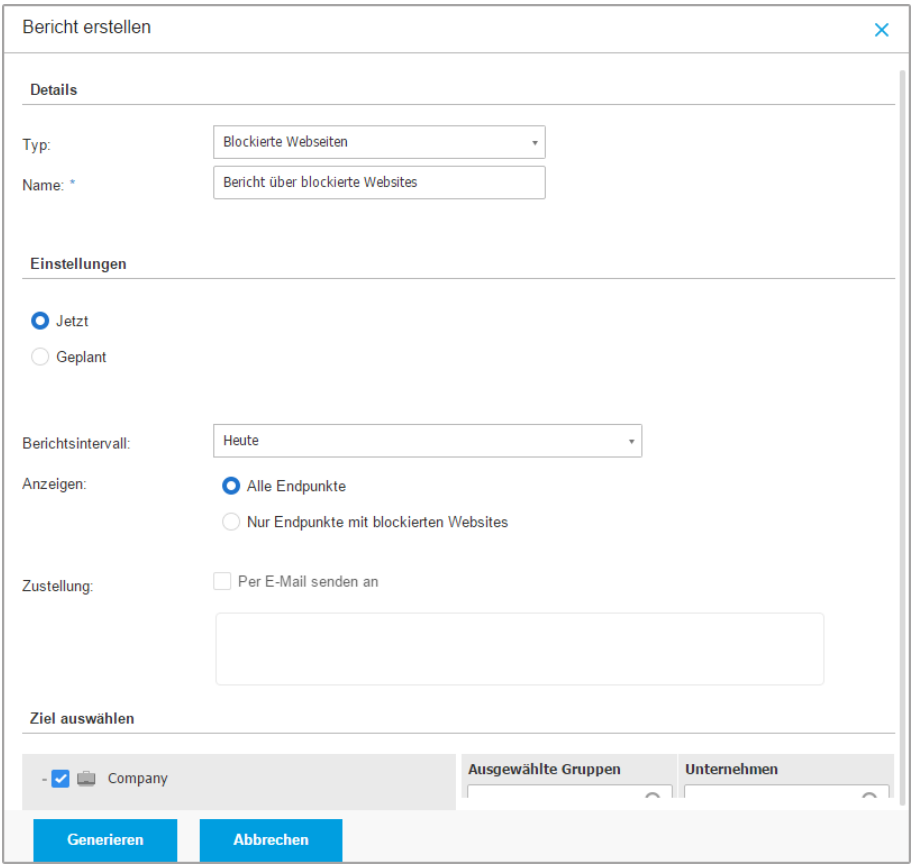
Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **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. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.



Berichtsoptionen

3. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus. Weitere Informationen finden Sie unter „Berichtstypen“ (S. 410)
4. 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.
5. 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).

6. 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.
7. 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.

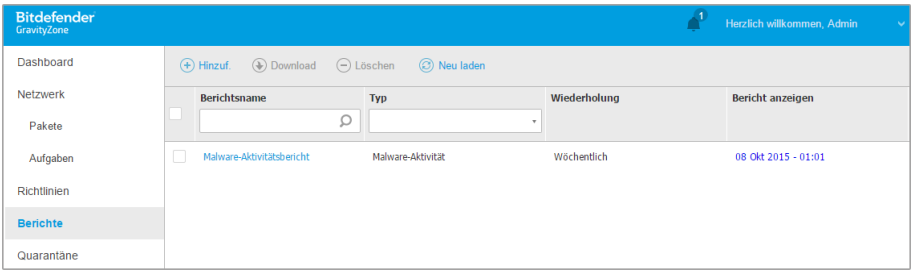
   Für einen **Update-Status**-Bericht können Sie zum Beispiel auf Wunsch nur die Netzwerkobjekte anzeigen, die nicht aktualisiert wurden, oder diejenigen, die neu gestartet werden müssen, um das Update abzuschließen.
8. **Zustellung**. Um einen geplanten Bericht als E-Mail geschickt zu bekommen, markieren 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.
9. **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.
10. 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.

11.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.



Die Berichteseite

Alle geplanten Berichte werden zusammen mit nützlichen Informationen zu den Berichten in einer Tabelle angezeigt:

- Name und Art des Berichts
- Berichtwiederholung
- 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**.

11.3.1. 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. 435)

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.

11.3.2. 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.

11.3.3. 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.

11.4. Berichtbasierte 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 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:

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.

11.5. 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

11.5.1. 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.

11.5.2. 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.

11.6. 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 Berichtnamen.
   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.

11.7. Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen. Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

12. QUARANTÄNE

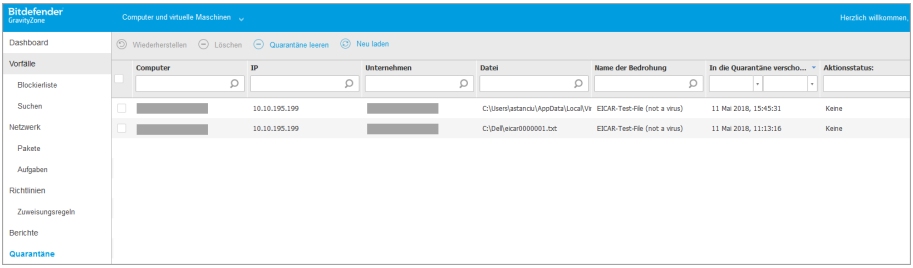
Die Quarantäne ist ein verschlüsselter Ordner, in dem potenziell bösartige Dateien aufbewahrt werden, so zum Beispiel vermutlich oder tatsächlich mit Malware infizierte Dateien und andere unerwünschte Dateien. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden, Viren 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.

Jeder Endpunkt hat seine eigene lokale Quarantäne.

12.1. 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.



Die Quarantäneübersicht

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.

12.2. 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. 188).

12.2.1. 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.

12.2.2. 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.

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. Markieren Sie die Kästchen für die Dateien in Quarantäne, die Sie wiederherstellen möchten.
3. Klicken Sie auf die Schaltfläche **Wiederherstellen** am oberen Rand der Tabelle.
4. 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.
5. 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.
6. Klicken Sie auf **Speichern**, um die Aktion zum Wiederherstellen einer Datei anzufordern. Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.
7. 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.

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:

1. 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. Markieren Sie die Kästchen für die Dateien in der Quarantäne, die Sie löschen möchten.
3. 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. Klicken Sie auf **Quarantäne leeren**.

Alle Einträge in der Quarantäne-Tabelle werden gelöscht. Die angeforderte Aktion wird sofort (bzw. sobald diese wieder online sind) an die entsprechenden Netzwerkobjekte geschickt.

12.3. 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.

12.3.1. 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 Qurantäne 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 **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 Qurantäne 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.

12.3.2. 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 im Kapitel „Ausschlüsse“ (S. 189).

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 15 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

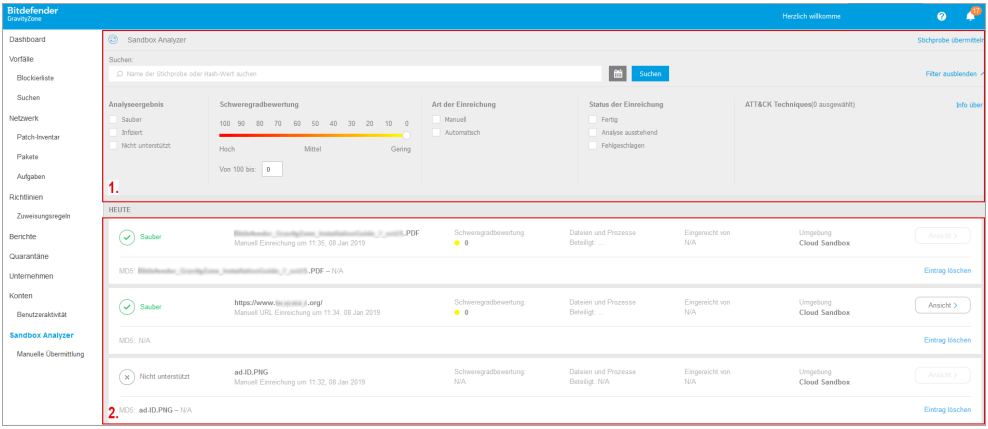
So löschen Sie alle Objekte in der Quarantäne:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Wählen Sie **Exchange** aus der Ansichtsauswahl.
3. Klicken Sie auf **Quarantäne leeren**.

Alle Einträge in der Quarantäne-Tabelle werden gelöscht. Die angeforderte Aktion wird sofort an die Ziel-Netzwerkobjekte übermittelt.

13. 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 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
- Übermittlungskarten löschen
- Manuelle Übermittlung vornehmen.

13.1. 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 Dateiendungen für die manuelle Übermittlung“ (S. 486).
- **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 Richtlinieneinstellungen an den Sandbox Analyzer 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.
- **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.

13.2. 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-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.

Wichtig
HTML-Berichte sind nur in Englisch verfügbar, unabhängig von der Sprache, die Sie für GravityZone Control Center festgelegt haben.

13.3. 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**.

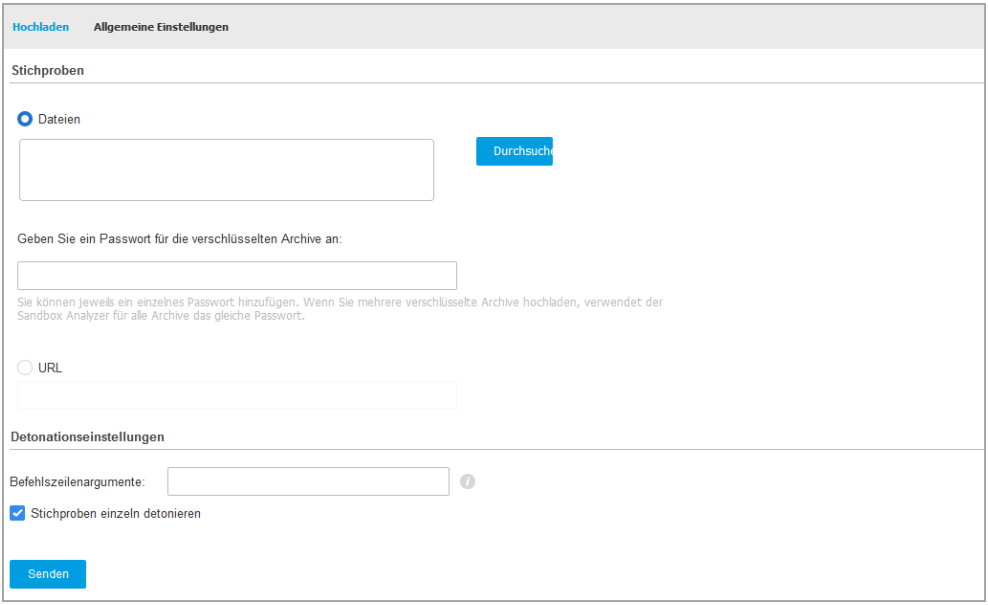
Beachten Sie
Auf diese Weise löschen Sie nur die Übermittlungskarte selbst. Alle Informationen zur Übermittlung sind auch weiterhin im Bericht **Sandbox Analyzer-Ergebnisse (veraltet)** verfügbar. Dieser Bericht wird jedoch nur noch eine begrenzte Zeit lang unterstützt.

13.4. 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.

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. 17)) am Control Center an.



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:

- **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.

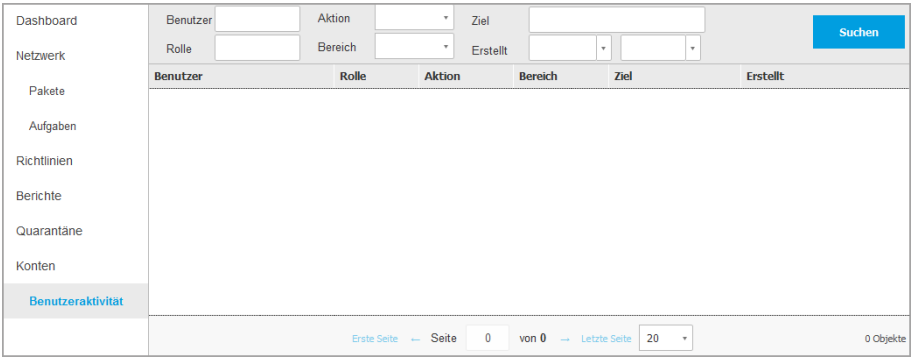
Beachten Sie
Zur manuellen Übermittlung an den Sandbox Analyzer müssen Sie über **Netzwerke verwalten**-Rechte verfügen.

14. 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
- Problembehandlungsvorgänge auf betroffenen Maschinen starten, beenden, abbrechen und anhalten
- Bearbeiten der Authentifizierungseinstellungen für die GravityZone-Benutzerkonten.

Details zu den Aktivitäten der Benutzer finden Sie auf der Seite **Konten > Benutzeraktivität**.



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.

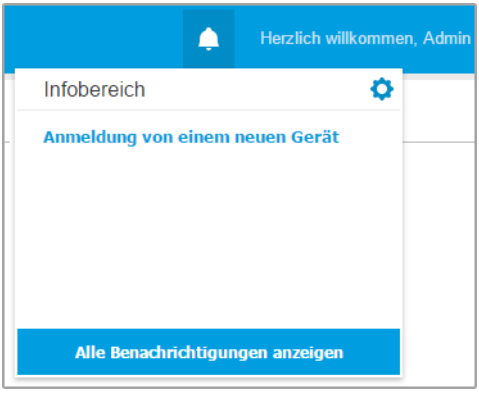
Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierungsreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

15. VERWENDUNG VON TOOLS

16. 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 11-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.

16.1. 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. 468).

Von HyperDetect gefundene Bedrohungen werden von dieser Benachrichtigung nicht abgedeckt.

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.

Lizenzobergrenze erreicht oder überschritten

Diese Benachrichtigung wird gesendet, wenn alle verfügbaren Lizenzen vergeben sind. Falls die Anzahl der Installationen die Lizenzgrenze überschreitet, zeigt die Benachrichtigung die nicht lizenzierten Endpunkte in der letzten 24 Stunden an.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

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.

Server-Lizenzobergrenze ist erreicht

Diese Benachrichtigung wird gesendet, wenn die Anzahl der geschützten Server die in Ihrem Lizenzschlüssel angegebene Obergrenze erreicht.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

Server-Lizenzobergrenze ist bald erreicht

Diese Benachrichtigung wird gesendet, wenn 90 % der verfügbaren Lizenzplätze für Server vergeben sind.

Sie benötigen die Berechtigung **Eigenes Unternehmen verwalten**, um diese Benachrichtigung zu sehen.

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.

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: CEF

Upgrade-Status

Diese Benachrichtigung wird wöchentlich ausgegeben, wenn alte Produktversionen in Ihrem Netzwerk gefunden werden.

Erweiterter Exploit-Schutz

Diese Benachrichtigung wird ausgegeben, wenn der erweiterte Exploit-Schutz Exploit-Versuche in Ihrem Netzwerk erkannt hat.

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: 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: 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: 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: CEF

Identitätsschutzereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn gemäß den Identitätsschutzregeln Datenverkehr auf einem Endpunkt blockiert wird.

Verfügbares syslog-Format: CEF

Produkt-Modul-Ereignis

Diese Benachrichtigung wird jedes Mal ausgegeben, wenn ein Sicherheitsmodul eines installierten Agenten aktiviert oder deaktiviert wird.

Verfügbares syslog-Format: 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: 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: CEF

Produktregistrierungsereignis

Diese Benachrichtigung informiert Sie darüber, wenn sich der Registrierungsstatus eines in Ihrem Netzwerk installierten Agenten geändert hat.

Verfügbares syslog-Format: 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.

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.

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.

Sie können diese Benachrichtigung auch für Scan-Aufgaben empfangen, die über NTSA ausgelöst wurden.

Verfügbares syslog-Format: CEF

Veralteter Update-Server

Diese Benachrichtigung wird gesendet, wenn die Sicherheitsinhalte auf einem Update-Server in Ihrem Netzwerk veraltet sind.

Verfügbares syslog-Format: 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.

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 Unternehmensname, 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 den von Ihrem Unternehmen übermittelten Stichproben finden Sie zudem im Bericht **Sandbox**

Analyzer-Ergebnisse (veraltet). Informationen zu den von Ihrem Unternehmen übermittelten Stichproben finden Sie zudem im Abschnitt **Sandbox Analyzer** im Control Center-Hauptmenü.

Verfügbares syslog-Format: CEF

HyperDetect-Aktivität

Mit dieser Benachrichtigung werden Sie informiert, wenn HyperDetect Malware-Schutz-Ereignisse oder aufgehobene Blockierungen im Netzwerk findet. Diese Benachrichtigung erfolgt für jedes HyperDetect-Ereignis. Sie enthält die folgenden Detailinformationen:

- Betroffener Endpunkt (Name, IP, installierter Agent)
- Malware-Typ und -Name
- Infizierter Dateipfad. Bei dateilosen Angriffen wird der Name der für den Angriff verwendeten ausführbaren Datei angezeigt.
- Infektionsstatus
- Der SHA256-Hash der ausführbaren Malware-Datei.
- Der Art des beabsichtigten Angriffs (gezielter Angriff, Grayware, Exploit, Ransomware, verdächtige Dateien und Netzwerkdatenverkehr)
- Erkennungsstufe (tolerant, normal, aggressiv)
- Zeitpunkt und Datum des Fundes

Verfügbares syslog-Format: CEF

Wenn Sie mehr Details zu der Infektion erfahren und den Ursachen weiter auf den Grund gehen möchten, können Sie auf der Seite **Benachrichtigungen** einen **HyperDetect-Aktivität**-Bericht erzeugen. Hierzu müssen Sie:

1. Klicken Sie im Control Center auf die Schaltfläche **Benachrichtigung**, um den Benachrichtigungsbereich zu öffnen.
2. Mit einem Klick auf den Link **Mehr anzeigen** am Ende einer Benachrichtigung können Sie die Seite **Benachrichtigungen** öffnen.
3. Klicken Sie in den Benachrichtigungsdetails auf die Schaltfläche **Bericht anzeigen**. Dadurch wird das Berichtskonfigurationsfenster geöffnet.
4. Hier können Sie den Bericht bei Bedarf konfigurieren. Weitere Informationen finden Sie im Kapitel „Berichte erstellen“ (S. 428).
5. Klicken Sie auf **Generieren**.

Beachten Sie
Um Sie nicht zu sehr zu stören, erhalten Sie maximal eine Benachrichtigung pro Stunde.

Problem mit der Active-Directory-Integration
Diese Benachrichtigung informiert Sie über Probleme, die die Synchronisation mit Active Directory beeinträchtigen.

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. Die Benachrichtigung wird an alle Ihre Benutzerkonten gesandt.

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: CEF

Neuer Vorfall (EDR)
Diese Benachrichtigung informiert Sie, wenn ein neuer Vorfall eintritt. Nach der Aktivierung wird die Benachrichtigung jedes Mal erzeugt, wenn ein neuer Vorfall im Abschnitt **Vorfälle** des Control Centers angezeigt wird. Für weitere Details klicken Sie auf den **Namen des Vorfalls**.

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 Zeitpunk 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.

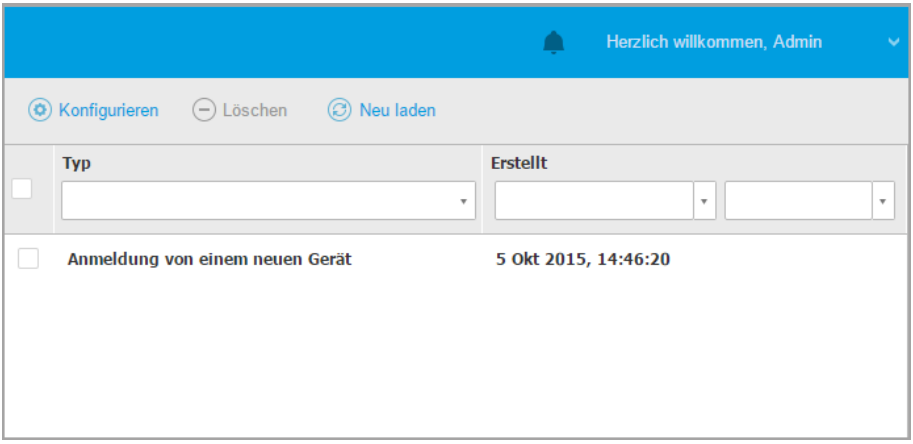
Verfügbares Syslog-Format: JSON, CEF

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.

16.2. 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.



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.

16.3. 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.

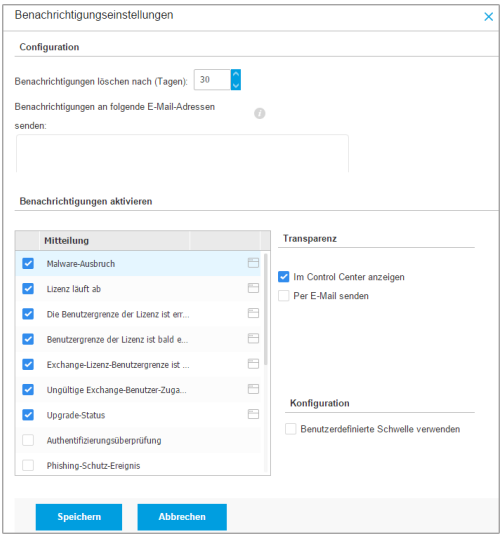
Sie können auch einstellen, dass Benachrichtigungen nach einer bestimmten Anzahl an Tagen gelöscht werden. Weitere Informationen finden Sie im Kapitel „Benachrichtigungseinstellungen konfigurieren“ (S. 468).

16.4. 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 **Benachrichtigungsseinstellungen** wird angezeigt.



Benachrichtigungseinstellungen

Beachten Sie
Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

3. Im Bereich **Konfiguration** können Sie die folgenden Einstellungen vornehmen:
   - Benachrichtigungen automatisch nach Ablauf einer bestimmten Zeit löschen. Eine beliebige Zahl zwischen 1 und 365 ins Feld **Benachrichtigungen nach (Tagen) löschen** eintragen.
   - 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`.
4. 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 im Kapitel „Benachrichtigungsarten“ (S. 460). 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.
- **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.
- 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**.

17. 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.

17.1. 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 berechtigen 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.

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.

17.2. Hilfe anfordern

Nutzen Sie unser Online-Support-Center, um Unterstützung anzufordern. Füllen Sie das Kontaktformular aus und senden Sie es ab.

17.3. 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.

17.3.1. 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.

17.3.2. 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 folgendem 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_Maschinenname_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 Systen, z. B. externe Verbindungen von Prozessen und CPU-Auslastung
- Systemprotokolle

17.3.3. 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 Administratorkennworts 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.

17.4. 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.

17.4.1. 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

17.4.2. 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.

17.4.3. 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
Webseite: 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
Webseite: 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
Webseite: 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
Webseite: 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
Webseite: 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; xlsm; 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
	Active-Directory-Integrator-Computer
	Exchange-Server-Computer
	Relais-Exchange-Server-Computer
	Virtuelle Maschine
	Relais-VM
	Golden Image
	Virtuelle Exchange-Server-Maschine
	Virtuelle Relais-Exchange-Server-Maschine
	Security Server

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
	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; xlsm; 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 SDatenverzeichnis 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. Sandbox Analyzer-Objekte

A.6.1. 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.6.2. Dateitypen, die durch die Vorfilterung von Inhalten bei der automatischen Übermittlung unterstützt werden

Die Vorfilterung der Inhalte bestimmt Dateitypen durch eine Kombination aus Objektinhalt und Dateiendung. Das bedeutet, dass eine ausführbare Datei mit der

Dateiendung `.tmp` als Anwendung erkannt und bei Verdacht an denSandbox Analyzer übermittelt wird.

- Anwendungen - Dateien im PE32-Format, einschließlich, aber nicht beschränkt auf die folgenden Dateiendungen: `exe, dll, com`.
- Dokumente - Dateien im Dokumentformat, einschließlich, aber nicht beschränkt auf die folgenden Dateiendungen: `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, psc1, jse, vbe`.
- Archive: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00`.
- E-Mails (im Dateisystem gespeichert): `eml, tnef`.

A.6.3. Standardausschlüsse bei automatischer Übermittlung

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

A.7. Datenerhebung zu menschlichen Risiken

Wir stellen sicher, dass sensible Daten ausschließlich vorübergehend und auf lokaler Ebene, d. h. auf dem Arbeitsplatzrechner des Benutzers, gesammelt und gespeichert werden. Dies dient dem alleinigen Zweck, Warnmeldungen über potenzielle Gefahren, denen Ihr Unternehmen durch das Benutzerverhalten ausgesetzt sein könnte, auszugeben. Wir speichern keine persönlichen Daten wie Klartext-Benutzernamen und Passwörter in Cloud-Datenbanken.

Die von uns gesammelten lokalen Daten werden regelmäßig gelöscht und dürfen nur Hashes von Benutzernamen und Passwörtern, die Gesamtzahl der riskanten Websites, auf die in einem bestimmten Zeitraum zugegriffen wurde, und die URLs einiger dieser verdächtigen Websites sowie deren Domänen-IP-Adressen enthalten.

Die folgende Tabelle gibt Auskunft darüber, welches Nutzerverhalten die ERA überwacht und wie sie Nutzerdaten verarbeitet und sammelt.

Name der Regel	Beschreibung	Typ	Gesammelte Daten
Plain-HTTP-Zugangsdaten	Überprüft, ob der Benutzer seit dem letzten Scan Zugangsdaten über unsichere HTTP-Verbindungen übermittelt hat.	Passwörter	Überprüft, ob der Benutzer dasselbe Passwort für mehrere externe Websites verwendet. Dieses Szenario wird aktiviert, wenn wir mindestens zwei externe Websites mit demselben Passwort finden.
Gemeinsam genutztes HTTP-Passwort extern	Wir prüfen, ob der Benutzer auf unsichere Websites (HTTP) zugreift, und speichern die Anzahl der aufgerufenen Websites und deren Zeitstempel.	Passwörter	Wir speichern den Hash der Passwörter (CRC32-Format), die auf externen Websites eingegeben wurden, sowie die aufgerufene(n) URL(s), die Domänen-IP-Adressen und den Benutzernamen. Die Speicherung erfolgt lokal.
Gemeinsam genutztes HTTP-Passwort extern und intern	Überprüft, ob der Benutzer dasselbe Passwort für interne und externe Websites verwendet.	Passwörter	Wir speichern den Hash der Passwörter (CRC32-Format), die auf externen Websites eingegeben wurden, sowie die aufgerufene(n) URL(s) und die Domänen-IP-Adressen. Die Speicherung erfolgt lokal.
Risikoreiches Surfen	Überprüft, ob der Benutzer seit dem letzten Scan Websites besucht hat, die als betrügerisch oder als Phishing-Sites eingestuft sind.	surfen	Wir speichern nur die Anzahl der mit hohem Risiko behafteten Websites und deren URLs während eines bestimmten Zeitraums. Die Speicherung erfolgt lokal.

Name der Regel	Beschreibung	Typ	Gesammelte Daten
	Dieses Szenario wird aktiviert, wenn die Anzahl der aufgerufenen unsicheren Websites den aktuellen Schwellenwert überschreitet.		
Hohe Fundzahl	Überprüft, ob der Benutzer seit dem letzten Scan einer hohen Zahl an Bedrohungen ausgesetzt war. Das Szenario wird aktiviert, wenn die Anzahl der Funde pro Benutzer den voreingestellten Schwellenwert überschreitet..	Funde	Wir speichern die Anzahl der Funde, die während eines bestimmten Zeitraums ausgelöst wurden. Die Speicherung erfolgt lokal.
Infektion eines Wechseldatenträgers	Überprüft, ob der Benutzer seit dem letzten Scan einer Bedrohung von einem Wechseldatenträger (z. B. USB-Stick, externe Festplatte) ausgesetzt war.	Funde	Wir speichern die Funde, die während eines bestimmten Zeitraums ausgelöst wurden sowie die Infektionsquelle (USB/CD/ISO-Datei). Die Speicherung erfolgt lokal.
SMB-Infektion	Überprüft, ob der Benutzer seit dem letzten Scan über einen im Netzwerk freigegebenen Ordner auf	Funde	Wir speichern Dateizugriffsereignisse in freigegebenen Ordnern oder Freigaben im Netzwerk. Die Speicherung erfolgt lokal.

Name der Regel	Beschreibung	Typ	Gesammelte Daten
	schädliche Dateien zugegriffen hat.		
Surf-Infektktion	Überprüft, ob der Benutzer seit dem letzten Scan schädliche URLs aufgerufen hat.	Funde	Wir speichern die schädlichen/verdächtigen URLs und zählen sie. Die Speicherung erfolgt lokal.
Hohe Anzahl von Funden im Zeitverlauf	Überprüft, ob der Benutzer während eines bestimmten Zeitraums einer besonders hohen Anzahl von Bedrohungen ausgesetzt ist.	Funde	Wir speichern die Anzahl der Infektionen während eines bestimmten Zeitraums. Die Speicherung erfolgt lokal.
Gemeinsam genutztes HTTP-Passwort extern	Überprüft, ob der Benutzer es versäumt, die Passwörter für externe Websites regelmäßig zu ändern.	Passwörter	Folgendes wird lokal gespeichert: Passwort-Hashes (CRC32-Format), Benutzernamen-Hashes und die URLs von externen Websites, die dieses Verhalten ausgelöst haben sowie Domänen-IP-Adressen.
Altes Benutzerpasswort	Überprüft, ob der Benutzer das Anmeldepasswort für das Konto (lokal oder Domain) seit mehr als 30 Tagen nicht geändert hat.	Passwörter	Wir speichern nichts lokal. Wir fragen eine Funktion von Active Directory ab, die zurückgibt, wann das letzte Mal das Kennwort für einen Benutzer geändert wurde.

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. Anderseits 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 Virenscanner 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 verbreitesten 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.

IOR

Risikoindikator - bezieht sich auf einen Registrierungsschlüsselwert oder Daten einer bestimmten Systemeinstellung oder eine bekannte App-Schwachstelle.

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 bösartiger 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 bösartige 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

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, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

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 bösartiges 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 schenkten. 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.

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.