Bitdefender

GravityZone

INSTALLATIONSANLEITUNG

Bitdefender GravityZone Installationsanleitung

Veröffentlicht 2021.01.12

Copyright© 2021 Bitdefender

Rechtlicher Hinweis

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

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

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

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

Inhaltsverzeichnis

Vorwort

Dieses Handbuch richtet sich an IT-Administratoren, die mit der Installation von GravityZone innerhalb ihres Unternehmens betraut sind. IT-Administratoren finden in diesem Handbuch Informationen zu GravityZone sowie zu den Installationsanforderungen und den in GravityZone verfügbaren Sicherheitsmodulen.

Hier wird erklärt, wie Bitdefender-Sicherheitsagenten auf verschiedenen Arten von Endpunkten in Ihrem Unternehmen installiert und wie GravityZone konfiguriert werden kann.

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. v)	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)

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 finden Sie im Kapitel „Unterstützte Betriebssysteme“ (S. 22).

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.

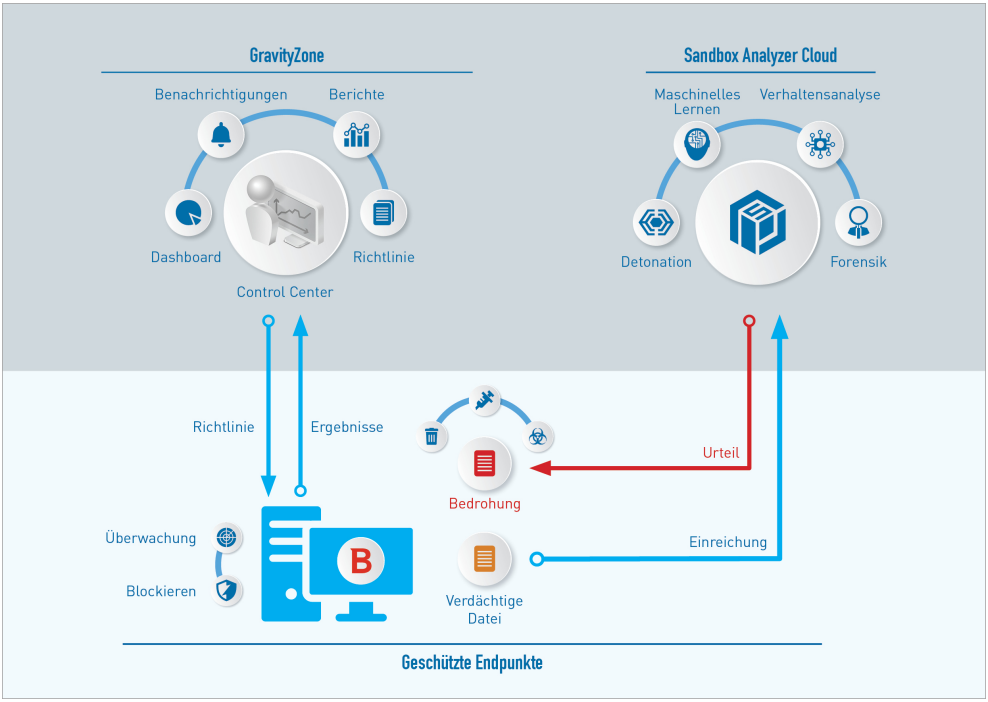
Der Sandbox Analyzer umfasst die folgenden Komponenten:

- **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.

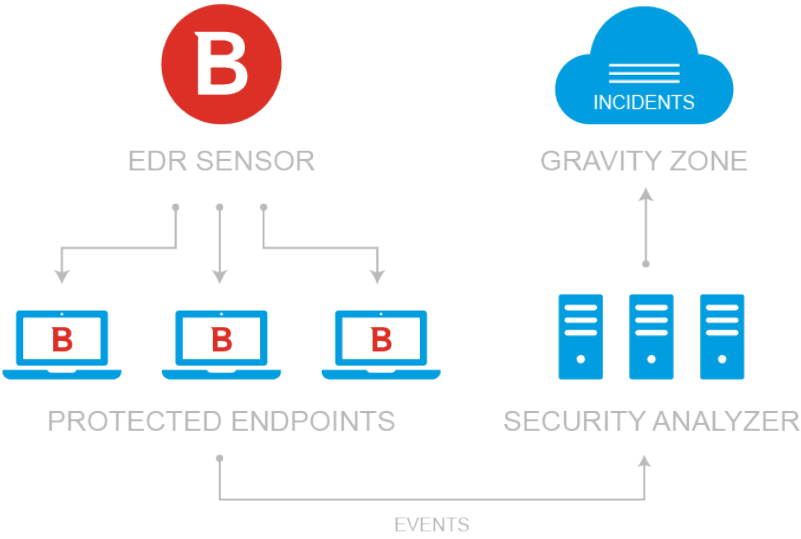
Die Analyseergebnisse werden mit ihrem Datei-Hash-Wert in der Sandbox Analyzer-Datenbank gespeichert. Wenn eine bereits zuvor analysierte Datei von einem anderen Endpunkt gemeldet wird, wird sofort eine Antwort zurückgegeben, da die Ergebnisse bereits in der Datenbank vorhanden sind.

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. ANFORDERUNGEN

Alle GravityZone-Lösungen werden über das Control Center installiert und verwaltet.

4.1. Control Center

Folgendes wird benötigt, um die Control Center-Web-Konsole aufzurufen:

- 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.

4.2. Endpunktschutz

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen die GravityZone-Sicherheitsagenten auf den Netzwerk-Endpunkten installiert werden. Für bestmöglichen Schutz können Sie auch Security Server installieren. Dazu benötigen Sie einen Control Center-Benutzer mit Administratorrechten für die Dienste, die Sie installieren möchten, und für die von Ihnen verwalteten Netzwerk-Endpunkte.

Die Anforderungen an den Sicherheitsagenten sind unterschiedlich, je nachdem, ob er zusätzliche Serverrollen wie Relais, Exchange-Schutz oder Patch-Cache-Server hat. Weitere Informationen zu den Rollen des Agenten finden Sie unter „Sicherheitsagenten“ (S. 10).

4.2.1. Hardware

Sicherheitsagent ohne Rollen

CPU-Ausl.

Zielsysteme	CPU-Typ	Unterstützte Betriebssysteme
Arbeitsplatzrechner	Mit Intel® Pentium kompatible Prozessoren, mindestens 2 GHz	Microsoft-Windows-Desktop-Betriebssystem
	Intel® Core 2 Duo, mindestens 2 GHz	macOS
Intelligente Geräte	Mit Intel® Pentium kompatible Prozessoren, mindestens 800 MHZ	Eingebettete Microsoft-Windows-Betriebssysteme
Server	Minimalanforderung: Mit Intel® Pentium kompatible Prozessoren, 2.4 GHz	Microsoft-Windows-Server- Betriebssysteme und Linux-Betriebssysteme
	Empfohlen: Intel® Xeon Multi-Core CPU, mindestens 1.86 GHz	

Warnung
ARM-Prozessoren werden derzeit nicht unterstützt.

Freier RAM

Bei Installation (MB)

BS	EINZELNE ENGINE					
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	k.A.	k.A.	k.A.	k.A.

Bei täglicher Nutzung (MB)*

BS	Virenschutz (Single Engine)			Schutzmodule				
	Lokal	Hybrid	Zentralisiert	Verhaltens -Scan	Firewall	Inhalts-Steuerung	Power-User	Update-Server
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Freier Festplattenspeicher

Bei Installation (MB)

BS	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100

BS	EINZELNE ENGINE						ZWEI ENGINES			
	Lokales Scan -Verfahren		Hybrid-Scan -Verfahren		Zentrales Scan -Verfahren		Zentrales + lokales Scan-Verfahren		Zentrales + Hybrid-Scan -Verfahren	
	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.	Nur AV	Voller Umf.
macOS	1024	1024	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.

Bei täglicher Nutzung (MB)*

BS	Virenschutz (Single Engine)			Schutzmodule				
	Lokal	Hybrid	Zentralisiert	Verhaltens -Scan	Firewall	Inhalts-Steuerung	Power-User	Update-Server
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Angegeben ist der Bedarf für die tägliche Nutzung des Endpunkt-Clients, ohne zusätzliche Aufgaben wie Bedarf-Scans oder Produkt-Updates.

Sicherheitsagent mit Relais-Rolle

Die Relay-Rolle benötigt über die Grundkonfiguration des Sicherheitsagenten hinausgehende weitere Hardware-Ressourcen. Diese Anforderungen dienen der Unterstützung des Update-Servers und der vom Endpunkt gehosteten Installationspakete:

Anzahl der verbundenen Endpunkte	CPU zur Update-Server-Unterstützung	RAM	Freier Speicherplatz für Update-Server
1-300	Mindestens Intel® Core™ i3 oder gleichwertiger Prozessor, 2 vCPU pro Kern	1.0 GB	10 GB

Anzahl der verbundenen Endpunkte	CPU zur Update-Server-Unterstützung	RAM	Freier Speicherplatz für Update-Server
300-1000	Mindestens Intel® Core™ i5 oder gleichwertiger Prozessor, 4 vCPU pro Kern	1.0 GB	10 GB

Warnung

- ARM-Prozessoren werden derzeit nicht unterstützt.
- Relais-Agente erfordern SSD-Festplatten, um die hohe Anzahl der Lese- und Schreibvorgänge unterstützen zu können.

Wichtig

- Wenn Sie die Installationspakete und Updates auf einer anderen Partition als der, auf der der Agent installiert ist, speichern möchten, stellen Sie sicher, dass beide Partitionen über ausreichend freien Speicherplatz (10 GB) verfügen, andernfalls bricht der Agent die Installation ab. Dies ist nur bei der Installation erforderlich.
- Auf Windows-Endpunkten müssen die symbolischen Links für lokal zu lokal aktiviert sein.

Sicherheitsagent mit Exchange-Schutz-Rolle

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.

Standardmäßig wird der Agent auf der Systempartition installiert.

Sicherheitsagent mit Patch-Cache-Server-Rolle

Der Agent mit der Patch-Cache-Server-Rolle muss alle der folgenden Anforderungen erfüllen:

- Alle Hardware-Anforderungen des einfachen Sicherheitsagenten (ohne Rollen)
- Alle Hardware-Anforderungen der Relais-Rolle
- Zusätzlich weitere 100 GB freier Speicherplatz zur Speicherung der heruntergeladenen Patches

Wichtig
Wenn Sie die Patches auf einer anderen Partition als der, auf der der Agent installiert ist, speichern möchten, stellen Sie sicher, dass beide Partitionen über ausreichend freien Speicherplatz (100 GB) verfügen, andernfalls bricht der Agent die Installation ab. Dies ist nur bei der Installation erforderlich.

4.2.2. Unterstützte Betriebssysteme

Windows Desktop

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows-10-Update vom . October 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Warnung
Bitdefender unterstützt keine Windows-Insider-Programm-Builds.

Windows-Tablet und Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux

Wichtig
Linux-Endpunkte verwenden Lizenzplätze aus dem Pool der Lizenzen für Server-Betriebssysteme.

- Ubuntu 14.04 LTS oder höher
- Red Hat Enterprise Linux / CentOS 6.0 oder höher(2)
- SUSE Linux Enterprise Server 11 SP 4 oder neuer
- OpenSUSE Leap 42.x
- Fedora 25 oder höher(1)
- Debian 8.0 oder höher
- Oracle Linux 6.3 oder höher
- Amazon Linux AMI 2016.09 oder höher
- Amazon Linux 2

Warnung
(1) Unter Fedora 28 (und neueren Versionen) muss für Bitdefender Endpoint Security Tools das Paket `libnsl` manuell installiert werden. Führen Sie dazu den folgenden Befehl aus:

```
sudo dnf install libnsl -y
```

(2) Bei Minimalinstallationen von CentOS muss für Bitdefender Endpoint Security Tools das Paket `libnsl` manuell installiert werden. Führen Sie dazu den folgenden Befehl aus:

```
sudo yum install libnsl
```

Voraussetzungen für Active Directory

Bei der Integration von Linux-Endpunkten mit einer Active-Directory-Domäne über den System Security Services Daemon (SSSD) müssen Sie darauf achten, dass die Tools **ldbsearch, krb5-user,** und **krb5-config** installiert sind und kerberos ordnungsgemäß konfiguriert ist.

```
/etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab
```

```
[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Beachten Sie
Es wird bei allen Eingaben zwischen Groß- und Kleinschreibung unterschieden.

Zugriff-Scan-Unterstützung

Zugriff-Scans sind auf allen unterstützten Gast-Betriebssystemen möglich. Auf Linux-Systemen werden Zugriff-Scans in den folgenden Fällen unterstützt:

Kernel-Versionen	Linux-Distributionen	Voraussetzungen für Zugriff-Scans
2.6.38 oder höher*	Red Hat Enterprise Linux / CentOS 6.0 oder höher Ubuntu 14.04 oder höher SUSE Linux Enterprise Server 11 SP 4 oder neuer OpenSUSE Leap 42.x Fedora 25 oder höher	**Fanotify** (Kernel-Option) muss aktiviert sein.

Kernel-Versionen	Linux-Distributionen	Voraussetzungen für Zugriff-Scans
	Debian 9.0 oder höher Oracle Linux 6.3 oder höher Amazon Linux AMI 2016.09 oder höher	
2.6.38 oder höher	Debian 8	**Fanotify** muss aktiviert und im „Enforcing"-Modus sein und anschließend das Kernel-Paket neu gebaut werden. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender bietet Support über **DazukoFS** mit vorgefertigten Kernel-Modulen an.
Alle anderen Kernel	Alle anderen unterstützten Systeme	Das **DazukoFS**-Modul muss manuell kompiliert werden. Weitere Informationen finden Sie unter „Kompilieren Sie das DazukoFS-Modul manuell" (S. 61).

* Mit bestimmten Einschränkungen (siehe unten).

Einschränkungen bei Zugriff-Scans

Kernel-Versionen	Linux-Distributionen	Details
2.6.38 oder höher	Alle unterstützten Systeme	Zugriff-Scans können nur unter folgenden Bedingungen zur Überwachung von gemounteten Netzwerkfreigaben eingesetzt werden: • **Fanotify** ist auf Remote- und lokalen Systemen aktiviert.

Kernel-Versionen	Linux-Distributionen	Details
		• Die Freigabe basiert auf dem CIFS- und NFS-Dateisystem. **Beachten Sie** Der Zugriff-Scan prüft keine Netzwerkfreigaben, die mit SSH oder FTP gemountet wurden.
Alle Kernel	Alle unterstützten Systeme	Auf Systemen mit **DazukoFS** werden Zugriff-Scans nicht für Netzwerkfreigaben unterstützt, die in Pfaden eingehängt sind, die bereits durch das Zugriff-Scan-Modul geschützt werden.

Unterstützung für Endpoint Detection and Response (EDR)

Eine vollständige und aktuelle Liste der Kernel-Versionen und Linux-Distributionen, die den EDR-Sensor unterstützen, finden Sie auf dieser Webseite.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Die Inhaltssteuerung wird von macOS Big Sur (11.0) nicht unterstützt.

4.2.3. Unterstützte Dateisysteme

Bitdefender kann auf den folgenden Dateisystemen installiert werden und diese schützen:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Beachten Sie
Bei NFS und CIFS/SMB werden Zugriff-Scans nicht unterstützt.

4.2.4. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.2.5. Security Server

Security Server ist eine vorkonfigurierte virtuelle Maschine, die auf einem Ubuntu Server 12.04 LTS (3.2-Kernel) läuft.

Virtualisierungsplattformen

Bitdefender Security Server kann auf den folgenden Virtualisierungsplattformen installiert werden:

- VMware vSphere & vCenter Server 7.0, 6.7 Update 3, Update 2a, 6.7 Update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  Beachten Sie
  Die Workload-Management-Funktionalität in vSphere 7.0 wird nicht unterstützt.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (einschließlich Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x

- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 oder Windows Server 2008 R2, 2012, 2012 R2 (inkl. Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inkl. KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism mit AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism mit AOS 5.6, 5.11 STS
- Nutanix Prism mit AHV 20170830.115, 20170830.301 und 20170830.395 Community Edition
- Nutanix Prism Version 2018.01.31 (Community Edition)

Beachten Sie
Der Support oder Virtualisierungsplattformen kann auf Anfrage bereitgestellt werden.

Arbeitsspeicher und CPU

Die Zuteilung der Arbeitsspeicher- und CPU-Ressourcen für den Security Server hängt von der Anzahl und Art der VMs ab, die auf dem Host laufen. In der folgenden Tabelle sind die empfohlenen Ressourcen aufgeführt:

Anzahl geschützter VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

Speicherplatz (Festplatte)

Sie müssen 8 GB Speicherplatz auf jedem Security Server-Host bereitstellen.

Security Server-Verteilung auf Hosts

Es ist zwar nicht zwingend erforderlich, aber Bitdefender empfiehlt, zur Verbesserung der Leistung Security Server auf jedem physischen Host zu installieren.

Netzwerklatenz

Die Kommunikationslatenz zwischen Security Server und den geschützten Endpunkten muss unter 50 ms liegen.

Speicherschutzlast

Der Speicherschutz wirkt sich bei einem Scan von 20 GB wie folgt auf den Security Server aus:

Status des Speicherschutzes	Security Server-Ressourcen	Security Server-Last	Übertragungszeit (mm:ss)
Deaktiviert (Baseline)	N/A	N/A	10:10
Aktiviert	4 vCPUs 4 GB RAM	Normal	10:30
Aktiviert	2 vCPUs 2 GB RAM	Hoch	11:23

Beachten Sie
Diese Ergebnisse wurden mit verschiedenen Typen von Musterdateien (.exe, .txt, .doc, .eml, .pdf, .zip etc.) zwischen 10 KB und 200 MB erzielt. Die Übertragungszeit entspricht 20 GB Daten in insgesamt 46.500 Dateien.

4.2.6. Bandbreitennutzung

- **Benötigte Bandbreite für Produkt-Updates zwischen dem Endpunkt-Client und dem Update-Server**

  Durch jedes regelmäßige Produkt-Update für Bitdefender Endpoint Security Tools entsteht der folgende Download-Datenverkehr an jedem Endpunkt-Client:

  - Unter Windows: ~20 MB
  - Unter Linux: ~26 MB
  - Unter macOS: ~25 MB

- **Datenverkehr für heruntergeladene Sicherheitsinhalte zwischen Endpunkt-Client und Update-Server (MB/Tag)**

Update-Server-Typ	Scan-Engine-Typ		
	Lokal	Hybrid	Zentrales
Relais	65	58	55
Öffentlicher Bitdefender-Update-Server	3	3.5	3

- **Für zentralisierte Scans benötigte Bandbreite zwischen dem Endpunkt-Client und dem Security Server**

Gescannte Objekte	Art des Datenverkehrs		Download (MB)	Upload (MB)
Dateien*	Erster Scan		27	841
	Gecachter Scan		13	382
Websites**	Erster Scan	Internet-Datenverkehr	621	N/A
		Security Server	54	1050
	Gecachter Scan	Internet-Datenverkehr	654	N/A
		Security Server	0.2	0.5

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

- **Hybrid-Scan-Datenverkehr zwischen dem Endpunkt-Client und Bitdefender Cloud Services.**

Gescannte Objekte	Art des Datenverkehrs	Download (MB)	Upload (MB)
Dateien*	Erster Scan	1.7	0.6
	Gecachter Scan	0.6	0.3
Internet-Datenverkehr**	Internet-Datenverkehr	650	N/A
	Bitdefender Cloud Services	2.6	2.7

* Die angegebenen Daten basieren auf einem Dateivolumen von 3,49 GB (6.658 Dateien), wovon 1,16 GB auf PE-Dateien (Portable Executable) entfallen.

** Die angegebenen Daten basieren auf den 500 bestbewerteten Websites.

Beachten Sie
Die Netzwerk-Latenz zwischen Endpunkt-Clients und Bitdefender Cloud Server muss unter 1 Sekunde liegen.

- **Datenverkehr zwischen Bitdefender Endpoint Security Tools Relay-Clients und Update-Server zum Herunterladen von Sicherheitsinhalten**

  Clients mit der Bitdefender Endpoint Security Tools Relay laden bei jedem unterstützten Betriebssystem ca. ~16 MB / Tag* vom Update-Server herunter.

  * Verfügbar für Bitdefender Endpoint Security Tools ab Version 6.2.3.569.

- **Datenverkehr zwischen Endpunkt-Clients und dem Control Center**

  Durchschnittlich entsteht pro Tag 618 KB an Datenverkehr zwischen Endpunkt-Clients und dem Control Center.

4.3. Exchange-Schutz

Security for Exchange wird durch Bitdefender Endpoint Security Tools bereitgestellt, das sowohl das Dateisystem als auch den Microsoft Exchange-Mail-Server schützt.

4.3.1. Unterstützte Microsoft-Exchange-Umgebungen

Security for Exchange unterstützt die folgenden Microsoft-Exchange-Versionen und -Rollen:

- Exchange Server 2019 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2016 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2013 mit Edge-Transport- oder Mailbox-Rolle
- Exchange Server 2010 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle
- Exchange Server 2007 mit Edge-Transport-, Hub-Transport- oder Mailbox-Rolle

Security for Exchange ist mit Microsoft-Exchange-Datenbankverfügbarkeitsgruppen kompatibel.

4.3.2. Systemanforderungen

Security for Exchange ist mit jedem physischen oder virtuellen 64-Bit-Server (Intel oder AMD) kompatibel, der eine unterstützte Microsoft-Exchange-Server-Version und -Rolle hat. Weitere Informationen zu Systemvoraussetzungen für Bitdefender Endpoint Security Tools finden Sie unter „Sicherheitsagent ohne Rollen“ (S. 18).

Empfohlene verfügbare Server-Ressourcen:

- Freier RAM: 1 GB
- Freier Festplattenspeicher: 1 GB

4.3.3. Andere Software-Anforderungen

- Für Microsoft Exchange Server 2013 mit Service Pack 1: KB2938053 von Microsoft.
- Für Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 oder neuer

4.4. Full Disk Encryption

GravityZone Full Disk Encryption ermöglicht es Ihnen, BitLocker auf Windows-Endpunkten und FileVault sowie das Befehlszeilenprogramm diskutil auf MacOS-Endpunkten über das Control Center zu betreiben.

Dieses Modul bietet durch vollständige Verschlüsselung fester bootfähiger und nicht-bootfähiger Laufwerke höchste Datensicherheit; außerdem speichert es Wiederherstellungsschlüssel für den Fall, dass ein Benutzer das Passwort vergisst.

Das Verschlüsselungsmodul nutzt die vorhandenen Hardware-Ressourcen in Ihrer GravityZone-Umgebung.

Softwareseitig sind die Anforderungen fast identisch mit denen für BitLocker, FileVault und dem Befehlszeilenprogramm diskutil, und die meisten Einschränkungen beziehen sich auf diese Tools.

Unter Windows

GravityZone-Verschlüsselung unterstützt BitLocker ab Version 1.2 auf Computern mit und ohne Trusted Platform Module (TPM)-Chip.

GravityZone unterstützt BitLocker auf Endpunkten mit den folgenden Betriebssystemen:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise

- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (mit TPM)
- Windows 7 Enterprise (mit TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (mit TPM)

*BitLocker ist in diesen Betriebssystemen nicht enthalten und muss separat installiert werden. Weitere Informationen zur Installation von BitLocker unter Windows Server finden Sie in den folgenden KB-Artikeln von Microsoft:

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

Wichtig
GravityZone unterstützt Verschlüsselung nicht unter Windows 7 und Windows 2008 R2 ohne TPM.

Details zu den Anforderungen für BitLocker finden Sie in folgendem KB-Artikel von Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Unter macOS

GravityZone unterstützt FileVault und diskutil auf macOS-Endpunkten mit den folgenden Betriebssystemen:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

- OS X El Capitan (10.11)

4.5. Speicherschutz

Unterstützte Speicher- und Filesharing-Lösungen:

- ICAP-kompatible Network Attached Storage (NAS)- und Storage Area Network (SAN)-Systeme von Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® und anderen Herstellern
- Nutanix® Files 3.x bis 3.6.2
- Citrix® ShareFile

4.6. GravityZone-Kommunikations-Ports

GravityZone ist eine dezentrale Lösung. Das bedeutet, dass die einzelnen Komponenten der Lösung über das lokale Netzwerk oder das Internet miteinander kommunizieren. Jede Komponente verwendet bestimmte Ports zur Kommunikation mit den anderen Komponenten. Diese Ports müssen für GravityZone offen sein.

Näheres zu GravityZone-Ports erfahren Sie in diesem Artikel.

5. SCHUTZ INSTALLIEREN

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die GravityZone-Sicherheitsagenten auf den Endpunkten installieren. Zu diesem Zweck benötigen Sie einen GravityZone Control Center-Benutzer mit Administratorrechten für die von Ihnen verwalteten Endpunkte.

5.1. Lizenzmanagement

GravityZone wird mit einem einzigen Schlüssel für alle Sicherheitsdienste lizenziert. Einzige Ausnahme ist Full Disk Encryption, für das es bei Jahreslizenzen einen separaten Schlüssel gibt.

Sie können GravityZone 30 Tage lang kostenlos testen. Während der Testphase stehen alle Funktionen uneingeschränkt zur Verfügung. Sie können den Dienst auf beliebig vielen Computern nutzen. Vor Ablauf der Testphase muss ein kostenpflichtiges Abonnement abgeschlossen werden, wenn Sie die Dienste ihn weiter nutzen möchten.

Wenn Sie eine Lizenz erwerben möchten, kontaktieren Sie einen Bitdefender-Händler, oder schreiben Sie uns eine E-Mail an enterprisesales@bitdefender.com.

5.1.1. Einen Händler finden

Unsere Händler stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl einer Lizenz-Option, die Ihren Anforderungen gerecht wird.

So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

1. Gehen Sie zur Partnersuche auf der Bitdefender-Website.
2. Wählen Sie Ihr Land, um Informationen zu Bitdefender-Partnern in Ihrer Nähe anzuzeigen.
3. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

5.1.2. Aktivieren Ihrer Lizenz

Beim ersten Abschluss eines kostenpflichtigen Abonnements erhalten Sie einen Lizenzschlüssel. Durch das Aktivieren dieses Lizenzschlüssels aktivieren Sie auch Ihr GravityZone-Abonnement.

Warnung
Die Aktivierung einer Lizenz überträgt deren Umfang NICHT auf die aktuelle Lizenz. Die alte Lizenz wird vielmehr durch die neue überschrieben. Wenn Sie zum Beispiel eine Lizenz für 10 Endpunkte über einer bestehenden Lizenz für 100 Endpunkte aktivieren, erhalten Sie KEIN Lizenzvolumen von 110 Endpunkten. Im Gegenteil, die Anzahl der lizenzierten Endpunkte sinkt von 100 auf 10.

Der Lizenzschlüssel wird Ihnen nach Erwerb per E-Mail zugesendet. Abhängig von Ihrer Dienstleistungsvereinbarung wird Ihr Dienstleister unter Umständen den freigegebenen Lizenzschlüssel für Sie aktivieren. Alternativ können Sie Ihre Lizenz auch manuell aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich über Ihr Konto am Control Center an.
2. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**.
4. Wählen Sie im Bereich **Lizenz** den **Lizenz**-Typ.
5. Geben Sie im Feld **Lizenzschlüssel** Ihren Lizenzschlüssel ein.
6. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
7. Geben Sie ins Feld **Add-on-Schlüssel** den Schlüssel für ein bestimmtes Add-on, z. B. für die Verschlüsselung, ein.
8. Klicken Sie auf **Hinzufügen**. Die Add-on-Details werden in der Tabelle angezeigt: Typ, Lizenzschlüssel sowie die Option, den Schlüssel zu entfernen.
9. Klicken Sie auf **Speichern**.
10. Um das Add-on nutzen zu können, müssen Sie sich zunächst vom Control Center abmelden und sich danach erneut anmelden. Im Anschluss können Sie in GravityZone auf die Add-on-Funktionen zugreifen.

5.1.3. Aktuelle Lizenzinformationen anzeigen

So zeigen Sie ihre Lizenzinformationen an:

1. Melden Sie mit Ihrer E-Mail-Adresse und dem per E-Mail zugesandten Passwort an der Control Center an.

5.2. Schutz für Endpunkte installieren

Je nach Konfiguration der Maschine und der Netzwerksumgebung können Sie entweder nur die Sicherheitsagenten installieren oder zusätzlich einen Security Server verwenden. Im letzeren Fall müssen Sie zuerst den Security Server installieren und dann erst die Sicherheitsagenten.

Es wird empfohlen, den Security Server zu verwenden, falls die Maschinen geringe Hardware-Resourcen haben.

Wichtig
Nur Bitdefender Endpoint Security Tools unterstützt die Verbindung zum Security Server. Weitere Informationen finden Sie im Kapitel „GravityZone-Architektur“ (S. 10).

5.2.1. Security Server installieren

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

Sie müssen Security Server auf einem oder mehreren Hosts installieren, um die entsprechende Anzahl an virtuellen Maschinen zu schützen.

Dazu müssen Sie die Anzahl der geschützten virtuellen Maschinen sowie die für Security Server auf den Hosts zur Verfügung stehenden Ressourcen und die Netzwerkverbindung zwischen Security Server und den geschützten virtuellen Maschinen bedenken.

Auf virtuellen Maschinen installierte Sicherheitsagenten stellen über TCP/IP eine Verbindung zum Security Server her. Dazu verwenden sie die Informationen, die bei der Installation oder über eine Richtlinie vorgegeben werden.

Download der Installationspakete für Security Server

So laden Sie Installationspakete für Security Server herunter:

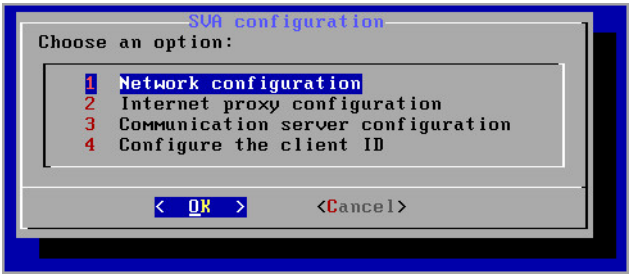
1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das Security Server-Standardpaket.
3. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Pakettyp aus dem Menü.
4. Speichern Sie das gewählte Paket am gewünschten Speicherort.

Einsatz von Security Server Installationspaketen

Sobald sie das Installationspaket haben, können Sie es auf dem Host mithilfe eines beliebigen Installationstools für virtuelle Maschinen installieren.

Richten Sie nach der Installation den Security Server wie folgt ein:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu. Alternativ können Sie auch über SSH eine Verbindung zur Appliance herstellen.
2. Melden Sie sich mit den Standardzugangsdaten an.
   - Benutzername: `root`
   - Passwort: `sve`
3. Führen Sie den Befehl `sva-setup` aus. Die Konfigurationsoberfläche der Appliance wird geöffnet.



Security Server-Konfigurationsoberfläche (Hauptmenü)

Verwenden Sie zur Navigation durch die Menüs und Optionen die `Tabulator`- und Pfeiltasten. Um eine bestimmte Option auszuwählen, drücken Sie `Enter`.

4. Konfigurieren Sie die Netzwerkeinstellungen.

   Der Security Server kommuniziert mit den anderen GravityZone-Komponenten über das TCP/IP-Protokoll. Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie im Hauptmenü den Punkt **Netzwerkkonfiguration**.

   b. Wählen Sie den Netzwerkadapter aus.

c. Wählen Sie den IP-Adressen-Konfigurationsmodus:

- **DHCP**, wenn Sie möchten, dass der Security Server die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht.
- **Statisch**, wenn kein DHCP-Server vorhanden ist oder wenn im DHCP-Server eine IP-Adresse für die Appliance reserviert wurde. In diesem Fall müssen Sie die Netzwerkeinstellungen manuell konfigurieren.

  i. Geben Sie Hostnamen, IP-Adresse, Netzwerkmaske, Gateway und DNS-Server in die entsprechenden Felder ein.

  ii. Wählen Sie **OK**, um die Änderungen zu speichern.

Beachten Sie
Wenn Sie über einen SSH-Client mit der Appliance verbunden sind, wird Ihre Sitzung sofort beendet, wenn Sie die Netzwerkeinstellungen ändern.

5. Konfigurieren Sie die Proxy-Einstellungen.

   Wenn im Netzwerk ein Proxy-Server verwendet wird, müssen Sie seine Details eingeben, damit der Security Server mit dem GravityZone Control Center kommunizieren kann.

   Beachten Sie
   Nur Proxy-Server mit Basic Authentication werden unterstützt.

   a. Wählen Sie im Hauptmenü den Punkt **Internet proxy configuration**.

   b. Geben Sie Hostnamen, Benutzernamen, Passwort und Domaine in die entsprechenden Felder ein.

   c. Wählen Sie **OK**, um die Änderungen zu speichern.

6. Konfigurieren Sie die Adresse des Kommunikationsservers.

   a. Wählen Sie im Hauptmenü den Punkt **Communication server configuration**.

   b. Geben Sie für den Kommunikationsserver die folgenden Adressen ein:

   - `https://cloud-ecs.gravityzone.bitdefender.com:443`
   - `https://cloudgz-ecs.gravityzone.bitdefender.com:443`

Wichtig
Diese Adresse muss die gleiche sein, die in den Richtlinieneinstellungen für Control Center erscheint. Zur Überprüfung des Links gehen Sie auf die Seite **Richtlinien**, ergänzen oder öffnen Sie eine benutzerdefinierte Richtlinie, navigieren Sie dann zum Bereich **Allgemein > Kommunikation > Kommunikationszuweisung für Endpunkte** und geben Sie den Namen des Kommunikationsservers in das Feld für die Spaltenüberschrift ein. Der richtige Server wird in den Suchergebnissen angezeigt.

c. Wählen Sie **OK**, um die Änderungen zu speichern.

7. Konfigurieren Sie die Client-ID.
   a. Wählen Sie aus dem Hauptmenü den Punkt **Client-ID konfigurieren**.
   b. Geben Sie die Unternehmens-ID ein.

      Die ID ist eine Folge von 32 Zeichen, die auf der Seite Unternehmensdetails im Control Center aufgeführt ist.
   c. Wählen Sie **OK**, um die Änderungen zu speichern.

5.2.2. Sicherheitsagent installieren

Um Ihre physischen und virtuellen Endpunkte zu schützen, müssen Sie auf jedem von ihnen einen Sicherheitsagenten installieren. Der Sicherheitsagent verwaltet den Schutz des lokalen Endpunkts. Zudem kommuniziert er mit dem Control Center, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Weitere Informationen zu verfügbaren Sicherheitsagenten finden Sie unter „Sicherheitsagenten“ (S. 10).

Auf Windows- und Linux-Maschinen kann der Sicherheitsagent zwei Rollen haben, und Sie können ihn wie folgt installieren:

1. Als einfachen Sicherheitsagenten für Ihre Endpunkte.
2. Als Relais, und somit als Sicherheitsagent und Kommunikations-, Proxy- und Update-Server für andere Endpunkte im Netzwerk.

Warnung
- Der erste Endpunkt, auf dem Sie den Schutz installieren, muss die Relais-Rolle haben, sonst können Sie den Sicherheitsagenten nicht per Fernzugriff auf anderen Endpunkten im selben Netzwerk installieren.

- Der Relais-Endpunkt muss eingeschaltet und online sein, damit die verbundenen Agenten mit dem Control Center kommunizieren können.

Sie können den Sicherheitsagenten auf physischen und virtuellen Endpunkten installieren, indem Sie Installationspakete lokal ausführen oder über Control Center Installationsaufgaben aus der Ferne ausführen.

Es ist wichtig, dass Sie die Anleitung sorgfältig lesen und befolgen, um die Installation richtig vorzubereiten.

Im Normalmodus haben die Sicherheitsagenten eine minimale Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Wenn der Netzwerkadministrator es per Installationspaket und Sicherheitsrichtlinie aktiviert hat, kann der Sicherheitsagent auf Windows-Endpunkten auch im Power-User-Modus ausgeführt werden. In diesem Modus kann der Endpunktbenutzer Sicherheitseinstellungen anzeigen und verändern. Der Control Center-Administrator kann jedoch in jedem Fall festlegen, welche Richtlinieneinstellungen angewendet werden und gegebenenfalls Einstellungen des Power-Users außer Kraft setzen.

Die Sprache der Benutzeroberfläche auf geschützten Windows-Endpunkten wird bei der Installation standardmäßig entsprechend der für Ihr GravityZone-Konto eingestellten Sprache festgelegt.

Auf Macs wird die Anzeigesprache der Benutzeroberfläche bei der Installation auf die Sprache festgelegt, auf die das Endpunktbetriebssystem eingestellt ist. Für Linux steht der Sicherheitsagent nicht in unterschiedlichen Sprachversionen zur Verfügung.

Um die Benutzeroberfläche auf bestimmten Windows-Endpunkten in einer anderen Sprache zu installieren, können Sie ein Installationspaket erstellen und die bevorzugte Sprache in den Konfigurationsoptionen dieses Pakets festlegen. Für Mac- und Linux-Endpunkte steht diese Option nicht zur Verfügung. Weitere Informationen zur Erstellung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 45).

Vor der Installation

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Endpunkte die Mindestsystemanforderungen erfüllen. Bei manchen Endpunkte kann es notwendig werden, das neueste Service Pack für das Betriebssystem zu installieren oder Speicherplatz zu schaffen. Legen Sie eine Liste der Endpunkte an, die die notwendigen Anforderungen nicht erfüllen, damit Sie diese von der Verwaltung ausschließen können.
2. Entfernen Sie alle bereits installierten Malware-Schutz- oder Internet-Sicherheits-Lösungen von den Endpunkten (eine Deaktivierung ist nicht ausreichend). Wenn der Sicherheitsagent gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies deren Funktion stören und massive Probleme auf dem System verursachen.

   Viele inkompatible Sicherheitsprogramme werden automatisch gefunden und bei der Installation des Sicherheitsagenten entfernt.

   Mehr zu diesem Thema und eine Liste von Sicherheitssoftware-Produkten, die Bitdefender Endpoint Security Tools auf aktuellen Windows-Betriebssystemen erkennt, finden Sie in diesem Artikel.

   Wichtig
   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.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Wenn sich die entsprechenden Endpunkte in einer Active-Directory-Domain befinden, müssen Sie zur Ferninstallation über Domainadministrator-Zugangsdaten verfügen. Befinden Sie sich nicht in einer Active-Directory-Domain, müssen Sie die Zugangsdaten für jeden einzelnen Endpunkt zur Hand haben.
4. Endpunkte müssen eine funktionierende Verbindung zum Control Center haben.
5. Für den Relais-Server wird die Nutzung einer statischen IP-Adresse empfohlen. Verwenden Sie den Host-Namen des Computers, falls Sie keine statische IP festlegen.
6. Wenn Sie den Agenten über ein Linux-Relais installieren, müssen zusätzlich 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.

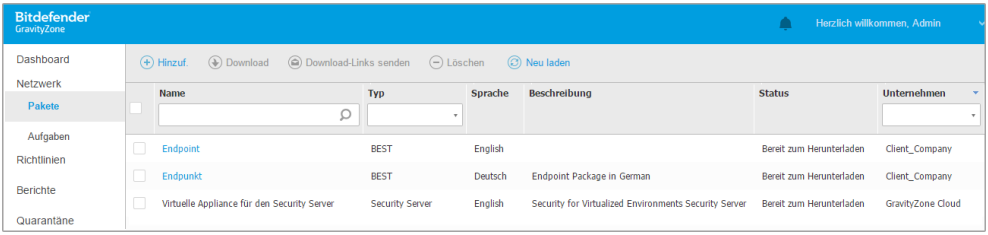
- Auf den gewünschten Windows-Endpunkten müssen Administratorfreigabe und Netzwerkfreigabe aktiviert sein.
- Für beteiligte Linux- und Mac-Endpunkte muss SSH aktiviert sein.

7. Nach der Installation von Endpoint Security for Mac (manuell oder aus der Ferne) unter macOS High Sierra (10.13) und neueren Betriebssystemversionen werden Benutzer aufgefordert, Bitdefender-Kernelerweiterungen auf ihren Computern zu genehmigen. Solange die Benutzer die Bitdefender-Kernelerweiterung noch nicht genehmigt haben, funktionieren einige Funktionen von Endpoint Security for Mac nicht. Um den Benutzern Aufwand zu ersparen, können die Bitdefender-Kernelerweiterungen auch im Voraus genehmigt werden, indem sie mithilfe eines Mobilgerät-Verwaltungstools auf die Whitelist gesetzt werden.

Lokale Installation

Eine Möglichkeit, den Sicherheitsagenten auf einem Endpunkt zu installieren ist es, ein Installationspaket lokal auszuführen.

Sie können die Installationspakete auf der Seite **Netzwerk > Pakete** erstellen und verwalten.



Die Paketübersicht

Warnung

- Die erste Maschine, auf der Sie den Schutz installieren, muss die Relais-Rolle haben, sonst können Sie den Sicherheitsagenten nicht auf anderen Endpunkten im Netzwerk installieren.
- Die Relais-Maschine muss eingeschaltet und online sein, damit die Clients mit dem Control Center kommunizieren können.

Nach der Installation des ersten Clients wird dieser dazu verwendet, um andere Endpunkte über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu finden. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 63).

Gehen Sie zur lokalen Installation des Sicherheitsagenten auf einem Computer folgendermaßen vor:

1. Sie können ein Installationspaket erstellen, das Ihren Anforderungen entspricht.

   Beachten Sie
   Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

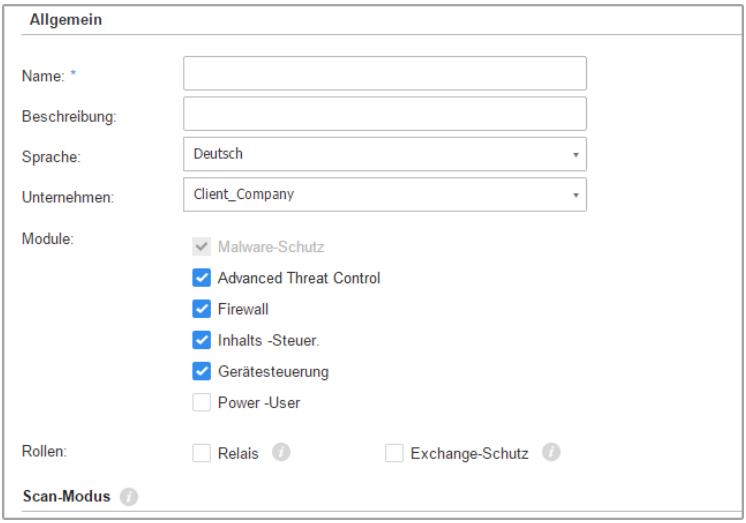
2. Auf diesem Endpunkt müssen Sie zunächst das Installationspaket herunterladen.

   Alternativ können Sie an mehrere Benutzer in Ihrem Netzwerk Download-Links zu den Installationspaketen per E-Mail senden.
3. Im nächsten Schritt Führen Sie das Installationspaket aus.

Installationspakete erstellen

So erstellen Sie ein Installationspaket:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird sich öffnen.



Pakete erstellen - Optionen

4. Geben Sie einen aussagekräftigen Namen und eine Beschreibung für das zu erstellende Installationspaket ein.
5. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.

   Beachten Sie
   Diese Option steht nur für Windows-Systeme zur Verfügung.

6. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.

   Beachten Sie
   Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden. Weitere Informationen finden Sie im Kapitel „Sicherheitsagenten“ (S. 10).

7. Wählen Sie die Rolle des gewünschten Endpunkts:
   - **Relais**, um das Paket für einen Endpunkt mit der Relais-Rolle zu erstellen. Weitere Informationen finden Sie unter „Relais“ (S. 12)

- **Patch-Management-Cache-Server**, um das Relais zu einem internen Server für die Verteilung von Software-Patches zu machen. Diese Rolle wird angezeigt, wenn die Relais-Rolle ausgewählt wird. Weitere Informationen finden Sie unter „Patch-Cache-Server“ (S. 12)
- **Exchange-Schutz**, um die Sicherheitsmodule für Microsoft-Exchange-Server zu installieren (Malware-Schutz, Spam-Schutz, Inhalts- und Anhangsfilter für den Exchange-E-Mail-Verkehr sowie Bedarf-Malware-Scans in Exchange-Datenbanken). Weitere Informationen finden Sie unter „Schutz für Exchange installieren“ (S. 67).

8. **Konkurrenzprodukte entfernen**. Es wird empfohlen, dieses Kästchen aktiviert zu lassen, um inkompatible Sicherheitssoftware automatisch zu entfernen, während der Bitdefender-Agent auf dem Endpunkt installiert wird. Wenn Sie diese Option deaktivieren, wird der Bitdefender-Agent zusätzlich zur bestehenden Sicherheitslösung installiert. Sie können die bereits installierte Sicherheitslösung zu einem späteren Zeitpunkt auf eigene Gefahr manuell entfernen.

   Wichtig
   Wenn der Bitdefender-Agent gleichzeitig mit anderen Sicherheitslösungen auf einem Endpunkt betrieben wird, kann dies deren Funktion stören und massive Probleme auf dem System verursachen.

9. **Scan-Modus**. Wählen Sie die Scan-Technologie, die am besten zu Ihrer Netzwerkumgebung und den Ressourcen Ihrer Endpunkte passt. Den Scan-Modus können Sie festlegen, indem Sie eine der folgenden Optionen wählen:

   - **Automatisch**. In diesem Fall erkennt der Sicherheitsagent automatisch die Konfiguration der entsprechenden Endpunkte und passt die Scan-Technologie daran an:
     - Zentralisierter Scan in der Public oder Private Cloud (mit Security Server) mit Ausweichmöglichkeit auf Hybrid-Scan (mit leichten Engines) für physische Computer mit geringer Hardware-Leistung und für virtuelle Maschinen. In diesem Fall muss mindestens ein Security Server im Netzwerk installiert sein.
     - Lokaler Scan (mit vollen Engines) für physische Computer mit hoher Hardware-Leistung.

Beachten Sie
Als Computer mit geringer Hardware-Leistung gelten Computer mit einer CPU-Frequenz von unter 1,5 GHz oder mit weniger als 1 GB RAM.

- **Benutzerdef**. In diesem Fall können Sie für physische und virtuelle Maschinen verschiedene Scan-Technologien festlegen:
  - Zentralisierter Scan in der Public oder Private Cloud (mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Full Engines) oder auf Hybrid-Scan (Light Engines)
  - Hybrid-Scan (mit leichten Engines)
  - Lokaler Scan (mit vollen Engines)

  Der Standard-Scan-Modus für EC2-Instanzen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre EC2-Instanzen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

  Der Standard-Scan-Modus für virtuelle Microsoft-Azure-Maschinen ist Lokaler Scan (Sicherheitsinhalte werden im installierten Sicherheitsagenten gespeichert, und der Scan wird lokal auf der Maschine ausgeführt). Wenn Sie Ihre virtuellen Microsoft-Azure-Maschinen mit einem Security Server scannen möchten, müssen Sie das Installationspaket des Sicherheitsagenten und die angewandte Richtlinie entsprechend konfigurieren.

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

  Weitere Informationen zu verfügbaren Scan-Technologien finden Sie hier:„Scan-Engines“ (S. 3)

10. Wenn Sie die Scan-Engines auf Public oder Private Cloud (Security Server) stellen, müssen Sie die lokal installierten Security Server, die Sie verwenden möchten, auswählen und ihre Priorität im Bereich **Security Server-Zuweisung** konfigurieren:
    a. Klicken Sie auf die Liste der Security Server in der Tabellenüberschrift. Die Liste der gefundenen Security Server wird angezeigt.

b. Wählen Sie eine Entität.

c. Klicken Sie in der Spaltenüberschrift **Aktionen** auf die Schaltfläche ⊕ **Hinzufügen**.

   Der Security Server wird der Liste hinzugefügt.

d. Wiederholen Sie diese Schritte, wenn Sie mehrere Security-Server hinzufügen möchten, falls es mehrere gibt. In diesem Fall können Sie ihre Priorität konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile (⌃ und ⌄) klicken. Wenn der erste Security Server nicht verfügbar ist, wird der nächste verwendet, und dann der nächste, usw.

e. Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⊗ **Löschen** am oberen Rand der Tabelle.

Sie können die Verbindung zum Security Server mit der Option **SSL verwenden** verschlüsseln.

11. Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Maschinen sauber sind, bevor Sie den Client auf ihnen installieren. Es wird dann ein Cloud-Schnell-Scan auf den Maschinen ausgeführt, bevor die Installation gestartet wird.

12. Bitdefender Endpoint Security Tools wird im Standard-Installationsverzeichnis installiert. Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie den Bitdefender-Agenten in einem anderen Ordner installieren möchten. Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.

    - Unter Windows lautet der Standardpfad `C:\Program Files\`. Wenn Sie Bitdefender Endpoint Security Tools in einem anderen Ordner installieren möchten, müssen Sie sich bei der Pfadbezeichnung an die Windows-Konventionen halten. Zum Beispiel `D:\Ordnername`.

    - Unter Linux wird Bitdefender Endpoint Security Tools standardmäßig im Ordner `/opt` installiert. Wenn Sie den Bitdefender-Agenten in einem anderen Ordner installieren möchten, müssen Sie sich bei der Pfadbezeichnung an die Linux-Konventionen halten. Zum Beispiel `/Ordnername`.

      Bei der Installation von Bitdefender Endpoint Security Tools sind folgende Pfade ausgeschlossen:

- an einem Pfad, der nicht mit einem Schrägstrich (/) beginnt; Die einzige Ausnahme hierzu ist der Windows-Pfad `%PROGRAMFILES%`, der vom Sicherheitsagenten als der Linux-Standardordner `/opt` interpretiert wird.
- Jeder Pfad, der sich unter `/tmp` oder `/proc` befindet.
- Jeder Pfad, der die folgenden Sonderzeichen enthält: `$, !, *, ?, ?, ", ', `, \, (,), [,], {, }`.
- Der `systemd`-Bezeichner (%).

Unter Linux wird für die Installationen an einem benutzerdefinierten Pfad mindestens glibc 2.21 benötigt.

Wichtig
Wenn Sie einen benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass Sie für jedes Betriebssystem das richtige Installationspaket verwenden.

13. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen. Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
14. Wenn sich die entsprechenden Endpunkte im Netzwerkinventar unter **Benutzerdefinierte Gruppen** befinden, können Sie sie direkt nach Abschluss der Installation des Sicherheitsagenten in einen anderen Ordner verschieben.

    Wählen Sie **Benutzerdefinierten Ordner verwenden**, und wählen Sie aus der entsprechenden Tabelle einen Ordner.
15. Wählen Sie im Bereich **Installer** die Entität, zu der die Endpunkte einer Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren.
    - **Bitdefender Cloud**, wenn Sie die Clients direkt aus dem Internet aktualisieren wollen.

      In diesem Fall können Sie auch die Proxy-Einstellungen definieren, wenn die Endpunkte ihre Internetverbindung über einen Proxy-Server herstellen. Wählen Sie **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in die entsprechenden Felder ein.
    - **Endpoint-Security-Relais** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Relais-Client verbinden möchten. Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie die gewünschte Relais-Maschine.

Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

Wichtig
Port 7074 muss offen sein, damit die Installation über einen Bitdefender Endpoint Security Tools Relay funktioniert.

16. Klicken Sie auf **Speichern**.

Das neu erstellte Paket wird zur Liste der Pakete hinzugefügt.

Beachten Sie
Die in einem Installationspaket konfigurierten Einstellungen werden sofort nach der Installation auf den jeweiligen Endpunkt angewendet. Sobald eine Richtlinie auf den Client angewendet wird, werden die Einstellungen dieser Richtlinie durchgesetzt und ersetzen gegebenenfalls die Einstellungen des Installationspakets (z. B. Kommunikationsserver oder Proxy-Einstellungen).

Installationspakete herunterladen

So laden Sie die Installationspakete der Sicherheitsagenten herunter:

1. Melden Sie sich über den Endpunkt, auf dem Sie die Software installieren möchten, am Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Installationspaket aus, das Sie herunterladen möchten.
4. Klicken Sie auf die Schaltfläche **Herunterladen** am oberen Rand der Tabelle und wählen Sie den Installer-Typ aus, den Sie verwenden möchten. Es gibt zwei Arten von Installationsdateien:
   - **Downloader**. Der Downloader lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.
   - **Installationspaket**. Die vollständigen Installationskits sind größer und sie müssen auf einem bestimmten Betriebssystem ausgeführt werden.

     Das vollständige Kit ist dafür da, um den Schutz auf Endpunkten mit einer langsamen bzw. keiner Internet-Verbindung zu installieren. Laden Sie diese

Datei auf einen mit dem Internet verbundenen Endpunkt herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe, um die Datei an andere Endpunkte weiterzugeben.

Beachten Sie
Verfügbare Installationspaket-Versionen:

- **Windows OS:** 32-Bit- und 64-Bit-Systeme
- **Linux OS:** 32-Bit- und 64-Bit-Systeme
- **macOS:** nur 64-Bit-Systeme

Vergewissern Sie sich, dass Sie die zum jeweiligen System passende Version wählen.

5. Speichern Sie die Datei auf dem Endpunkt.

Warnung

- Die Downloader-Datei darf nicht umbenannt werden, da sonst die Installationsdateien nicht vom Bitdefender-Server heruntergeladen werden können.

6. Zusätzlich können Sie, wenn Sie den Downloader gewählt haben, ein MSI-Paket für Windows-Endpunkte erstellen. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

Download-Links zu den Installationspaketen per E-Mail senden

Vielleicht möchten Sie andere Benutzer schnell darüber informieren, dass ein Installationspaket zum Download bereitsteht. Gehen Sie dazu wie folgt vor:

1. Gehen Sie zur Seite **Netzwerk > Pakete**.
2. Wählen Sie das gewünschte Installationspaket.
3. Klicken Sie auf die Schaltfläche **Download-Links senden** am oberen Rand der Tabelle. Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adressen aller Benutzer ein, die den Download-Link zum Installationspaket erhalten sollen. Drücken Sie nach jeder E-Mail-Adresse die `Eingabetaste`.

   Vergewissern Sie sich, dass alle eingegebenen E-Mail-Adressen gültig sind.

5. Wenn Sie die Download-Links anzeigen möchten, bevor Sie sie per E-Mail versenden, klicken Sie auf die Schaltfläche **Installationslinks**.
6. Klicken Sie auf **Senden**. An jede eingegebene E-Mail-Adresse wird eine E-Mail mit dem Download-Link gesendet.

Installationspakete ausführen

Damit die Installation erfolgreich durchgeführt werden kann, muss das Installationspaket mit Administratorrechten ausgeführt werden.

Je nach Betriebssystem gestaltet sich die Installation des Pakets etwas unterschiedlich:

- Unter Windows und macOS:
  1. Laden Sie die Installationsdatei vom Control Center auf den gewünschten Endpunkt herunter oder kopieren Sie sie von einer Netzwerkfreigabe.
  2. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
  3. Führen Sie die ausführbare Datei aus.
  4. Folgen Sie den Instruktionen auf dem Bildschirm.

  Beachten Sie
  Nach der Installation von Endpoint Security for Mac unter macOS werden die Benutzer aufgefordert, Bitdefender-Kernelerweiterungen auf ihren Computern zu genehmigen. Einige Funktionen des Sicherheitsagenten funktionieren erst, wenn die Bitdefender-Kernelerweiterungen genehmigt wurden. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.

- Unter Linux:
  1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
  2. Laden Sie die Installationsdatei auf den gewünschten Endpunkt herunter oder kopieren Sie sie dorthin.
  3. Wenn Sie das vollständige Kit heruntergeladen haben, extrahieren Sie die Dateien aus dem Archiv.
  4. Verschaffen Sie sich Root-Rechte, indem Sie den Befehl `sudo su` ausführen.

5. Verändern Sie die Rechte für die Installationsdatei, damit Sie sie ausführen können:

```
# chmod +x installer
```

6. Führen Sie die Installationsdatei aus:

```
# ./installer
```

7. Um zu überprüfen, ob der Agent auf dem Endpunkt installiert wurde, können Sie diesen Befehl ausführen:

```
$ service bd status
```

Einige Minuten nachdem der Sicherheitsagent installiert wurde, wird der Endpunkt im Control Center (**Netzwerk**-Seite) als verwaltet angezeigt.

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.

Remote-Installation

Mit Control Center können Sie den Sicherheitsagenten über Installationsaufgaben aus der Ferne auf Endpunkten installieren, die im Netzwerk gefunden wurden.

Nachdem Sie den ersten Client mit Relais-Rolle lokal installiert haben, kann es einige Minuten dauern, bis die anderen Netzwerk-Endpunkte im Control Center angezeigt werden. Von hier an können Sie den Sicherheitsagenten per Fernzugriff auf Endpunkten, die Sie verwalten, mithilfe der Installationsaufgaben im Control Center installieren.

Bitdefender Endpoint Security Tools verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem andere Endpunkte im gleichen Netzwerk gefunden werden können. Gefundene Endpunkte werden als **Nicht verwaltet** auf der **Netzwerk**-Seite angezeigt.

Damit die Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools bereits auf mindestens einem Endpunkt im Netzwerk installiert haben. Dieser Endpunkt wird dann verwendet, um das Netzwerk zu scannen und Bitdefender Endpoint Security Tools auf den noch nicht geschützten Endpunkten zu installieren.

Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 63).

Anforderungen für die Ferninstallation

Damit die Ferninstallation funktioniert, müssen die folgenden Punkte gegeben sein:

- Bitdefender Endpoint Security Tools Relay muss in Ihrem Netzwerk installiert sein.
- Unter Windows:
  - Die administrative Freigabe `admin$` muss aktiviert sein. Konfigurieren Sie jeden Zielarbeitsplatzrechner so, dass die erweiterte Freigabe von Dateien nicht verwendet wird.
  - Konfigurieren Sie die Benutzerkontensteuerung abhängig vom Betriebssystem, das auf den Endpunkten läuft. Wenn die Endpunkte in einer Active-Directory-Domain sind, können Sie die Benutzerkontensteuerung über eine Gruppenrichtlinie konfigurieren. Weitere Einzelheiten finden Sie in diesem Artikel in der Wissensdatenbank.

– Deaktivieren Sie die Windows-Firewall oder konfigurieren Sie sie so, dass Datenverkehr über das Datei- und Druckerfreigabeprotokoll zugelassen wird.

Beachten Sie
Die Ferninstallation funktioniert nur auf neueren Betriebssystemen ab Windows 7 / Windows Server 2008 R2, die Bitdefender vollständig unterstützt. Weitere Informationen finden Sie im Kapitel „Unterstützte Betriebssysteme“ (S. 22).

- Unter Linux: SSH muss aktiviert sein.
- Unter macOS: Remote-Anmeldung und Dateifreigaben müssen aktiviert sein.

Ausführen von Ferninstallationsaufgaben

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.

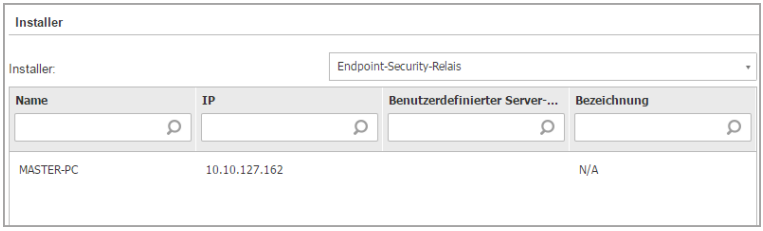
9. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.

   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:

    - Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der Tabelle im Bereich **Installer** aufgeführt. Jeder neue Client muss mit mindestens einem Relais-Client desselben Netzwerks verbunden sein, der als Kommunikations- und Update-Server fungiert. Wählen Sie das Relais, das Sie mit den gewünschten Endpunkten verknüpfen möchten. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

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

    - Wenn die Zielendpunkte über einen Proxy mit dem Relais-Agenten kommunizieren, müssen Sie auch die Proxy-Einstellungen festlegen. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.

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 Änderung von Installationspaketen finden Sie unter „Installationspakete erstellen“ (S. 45).

    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.

Linux-System für Zugriff-Scans vorbereiten

In Bitdefender Endpoint Security Tools für Linux können Zugriff-Scans durchgeführt werden. Dies funktioniert allerdings nur bei bestimmten Linux-Distributionen und Kernel-Versionen. Weitere Details erfahren Sie unter Systemvoraussetzungen.

Im nächsten Schritt lernen Sie, wie man das DazukoFS-Modul manuell kompiliert.

Kompilieren Sie das DazukoFS-Modul manuell

Gehen Sie wie unten beschrieben vor, um DazukoFS für die Kernel-Version des Systems zu kompilieren und laden Sie danach das Modul:

1. Laden Sie die geeigneten Kernel-Header herunter.
   - Führen Sie auf **Ubuntu**-Systemen den folgenden Befehl aus:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - Führen Sie auf **RHEL/CentOS**-Systemen den folgenden Befehl aus:

     ```
     $ sudo yum install kernel-devel kernel-headers-`uname -r`
     ```

2. Auf **Ubuntu**-Systemen benötigen Sie das Paket `build-essential`:

   ```
   $ sudo apt-get install build-essential
   ```

3. Kopieren und extrahieren Sie den DazukoFS-Quellcode in einem Verzeichnis Ihrer Wahl:

   ```
   # mkdir temp
   # cd temp
   # cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
   # tar -xzvf dazukofs-source.tar.gz
   # cd dazukofs-3.1.4
   ```

4. Kompilieren Sie das Modul:

   ```
   # make
   ```

5. Installieren und laden Sie das Modul:

   ```
   # make dazukofs_install
   ```

Voraussetzungen für Zugriff-Scans mit DazukoFS

Damit DazukoFS und Zugriff-Scans zusammen funktionieren, müssen die folgenden Voraussetzungen erfüllt sein. Vergewissern Sie sich das die folgenden Punkte auf Ihr Linux-System zutreffen und befolgen Sie die Anweisungen, um Probleme zu vermeiden.

- Die SELinux-Richtlinie muss deaktiviert oder auf **tolerant** gestellt sein. Sie können die Einstellungen der SELinux-Richtlinie einsehen und anpassen, indem Sie die Datei `/etc/selinux/config` bearbeiten.
- Bitdefender Endpoint Security Tools ist ausschließlich mit der Version von DazukoFS kompatibel, die im Installationspaket enthalten ist. Wenn DazukoFS auf Ihrem System bereits installiert ist, muss es vor der Installation von Bitdefender Endpoint Security Tools entfernt werden.
- DazukoFS unterstützt bestimmte Kernel-Versionen. Wenn das in Bitdefender Endpoint Security Tools enthaltene DazukoFS-Paket nicht mit der Kernel-Version des Systems kompatibel ist, kann das Modul nicht geladen werden. Ist das der Fall, können Sie den Kernel auf die unterstützte Version aktualisieren oder das DazukoFS-Modul für Ihre Kernel-Version rekompilieren. Das DazukoFS-Paket befindet sich im Installationsverzeichnis von Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Wenn Sie für Dateifreigaben dedizierte Server wie NFS, UNFSv3 oder Samba verwenden, müssen Sie die Dienste in der folgenden Reihenfolge starten:

  1. Aktivieren Sie im Control Center Zugriff-Scans per Richtlinie.

     Weitere Informationen hierzu finden Sie im GravityZone-Administratorhandbuch.

  2. Starten Sie den Dienst für die Netzwerkfreigabe.

     Für NFS:

     ```
     # service nfs start
     ```

     Für UNFSv3:

     ```
     # service unfs3 start
     ```

Für Samba:

```
# service smbd start
```

Wichtig
Beim NFS-Dienst ist DazukoFS nur mit dem NFS-User-Server kompatibel.

Wie die Netzwerkerkennung funktioniert

Neben der Integration mit Active Directory verfügt GravityZone über automatische Netzwerkerkennungsmechanismen zur Erkennung von Arbeitsgruppen-Computern.

GravityZone nutzt den **Microsoft-Computersuchdienst** und das Tool **NBTscan** für die Netzwerkerkennung.

Der Computersuchdienst ist eine Netzwerktechnologie, die auf Windows-basierten Computern zum Einsatz kommt, um immer aktuelle Listen von Domänen, Arbeitsgruppen und den Computern darin zu verwalten und diese Listen bei Bedarf an Client-Computer weiterzugeben. Computer, die über den Computersuchdienst im Netzwerk erkannt wurden, können durch Eingabe des **Net View**-Befehls im Eingabeaufforderungsfenster angezeigt werden.

Der Net-View-Befehl

Das Tool NBTscan scannt Computernetzwerke mit NetBIOS. Es fragt jeden Endpunkt im Netzwerk ab und sammelt Informationen wie IP-Adresse, NetBIOS-Computername und MAC-Adresse.

Damit die automatische Netzwerkerkennung funktioniert, müssen Sie Bitdefender Endpoint Security Tools Relay bereits auf mindestens einem Computer im Netzwerk installiert haben. Von diesem Computer aus wird das Netzwerk gescannt.

Wichtig

Das Control Center verwendet keine Netzwerkinformationen von Active Directory oder aus der Netzwerkübersicht. Die Netzwerkübersicht nutzt eine andere Technologie zur Netzwerkerkennung: das Link-Layer-Topology-Discovery-Protokoll (LLTD).

Control Center übernimmt keine aktive Rolle bei der Ausführung des Computersuchdienstes. Bitdefender Endpoint Security Tools fragt beim Computersuchdienst lediglich die Liste der aktuell im Netzwerk sichtbaren Arbeitsplatzrechner und Server ab (die Suchliste) und leitet diese dann an das Control Center weiter. Das Control Center verarbeitet die Suchliste und fügt neu erkannte Computer zur der Liste der **nicht verwalteten Computer** hinzu. Bereits erkannte Computer werden nach einer Netzwerkerkennungsabfrage nicht gelöscht, daher müssen Computer, die sich nicht mehr länger im Netzwerk befinden, manuell ausgeschlossen und gelöscht werden.

Die erste Abfrage der Suchliste wird vom ersten im Netzwerk installierten Bitdefender Endpoint Security Tools durchgeführt.

- Falls das Relais auf einem Arbeitsgruppen-Computer installiert wurde, werden im Control Center nur die Computer dieser Arbeitsgruppe angezeigt.
- Falls das Relais auf einem Domänen-Computer installiert wurde, werden im Control Center nur die Computer dieser Domäne angezeigt. Computer aus anderen Domänen können erkannt werden, wenn eine Vertrauensstellung mit der Domäne besteht, in der das Relais installiert ist.

Nachfolgende Netzwerkerkennungsabfragen werden danach stündlich wiederholt. Bei jeder neuen Abfrage teilt das Control Center die verwalteten Computer in Sichtbarkeitsbereiche auf und bestimmt in jedem Bereich ein Relais zur Durchführung der Aufgabe. Ein Sichtbarkeitsbereich ist eine Gruppe von Computern, die sich gegenseitig erkennen. Normalerweise wird ein Sichtbarkeitsbereich anhand einer Arbeitsgruppe oder Domäne definiert, im Einzelfall hängt dies jedoch von der Netzwerktopologie und Konfiguration ab. Unter Umständen besteht ein Sichtbarkeitsbereich auch aus mehreren Domänen oder Arbeitsgruppen.

Falls ein ausgewähltes Relais die Abfrage nicht durchführt, wartet das Control Center auf die nächste geplante Abfrage, ohne ein anderes Relais für einen weiteren Versuch auszuwählen.

Um das gesamte Netzwerk sichtbar zu machen, muss das Relais auf mindestens einem Computer in jeder Arbeitsgruppe oder Domäne in Ihrem Netzwerk installiert

sein. Im Idealfall sollte Bitdefender Endpoint Security Tools auf mindestens einem Computer in jedem Subnetzwerk installiert sein.

Weitere Informationen zum Microsoft-Computersuchdienst

Der Computersuchdienst auf einen Blick:

- Funktioniert unabhängig von Active Directory.
- Läuft ausschließlich über IPv4-Netzwerken und funktioniert unabhängig innerhalb der Grenzen einer LAN-Gruppe (Arbeitsgruppe oder Domäne). Eine Suchliste wird für jede LAN-Gruppe erstellt und verwaltet.
- Nutzt für die Kommunikation zwischen den Knoten üblicherweise verbindungslose Server-Übertragungen.
- Nutzt NetBIOS über TCP/IP (NetBT).
- Benötigt NetBIOS-Namensauflösung. Es wird empfohlen im Netzwerk eine Windows-Internet-Name-Service-Infrastruktur (WINS) zu unterhalten.
- Ist standardmäßig nicht in Windows Server 2008 und 2008 R2 aktiviert.

Weitere Informationen zum Computersuchdienst finden Sie in der Computer Browser Service Technical Reference im Microsoft Technet.

Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über das Control Center verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein. Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein. Die lokale Firewall muss NetBT-Verkehr zulassen.
- Wenn Sie mit einem Linux-Relais andere Linux- oder Mac-Endpunkte erkennen möchten, müssen Sie entweder auf den Zielendpunkten Samba installieren oder sie in einem Active Directory zusammenfassen und DHCP verwenden. Damit wird NetBIOS automatisch auf ihnen konfiguriert.

- Die Freigabe von Dateien muss auf den Computern aktiviert sein. Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.
- Die Netzwerkerkennung muss aktiviert sein (**Systemsteuerung (> Netzwerk und Internet) > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktionen nutzen zu können, müssen die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost
- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Bitdefender Endpoint Security Tools den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.

Beachten Sie
Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.

5.3. Installation von EDR

Dieses Modul ist standardmäßig im Installationskit für Bitdefender Endpoint Security Tools enthalten. Bei der ersten Eingabe des Lizenzschlüssels muss der Vorfallsensor aktiviert werden.

Stellen Sie vor der Installation sicher, dass die Zielendpunkte die Mindestanforderungen erfüllen. Die Vorfall-Mindestanforderungen entsprechen den Anforderungen für den Sicherheitsagenten.

Zum Schutz Ihrer Endpunkte mit EDR stehen Ihnen zwei Optionen zur Auswahl:

- Installieren Sie die Sicherheitsagenten mit dem EDR-Sensor, wenn Sie Ihren Lizenzschlüssel eingeben. Mehr dazu unter Aktivieren der Lizenz.
- Verwenden Sie die Aufgabe **Neu konfigurieren**.

Wichtig
The Incidents Sensor no longer provides support for Internet Explorer.

Weitere Informationen hierzu finden Sie im GravityZone-Administratorhandbuch.

5.4. Full Disk Encryption installieren

Full Disk Encryption muss über einen Lizenzschlüssel aktiviert werden.

Weitere Informationen zu Lizenzschlüsseln finden Sie hier: „Lizenzmanagement“ (S. 36).

Der Bitdefender-Sicherheitsagent unterstützt Full Disk Encryption ab Version 6.2.22.916 unter Windows und ab Version 4.0.0173876 unter macOS. Um sicherzugehen, dass die Agenten vollständig mit diesem Modul kompatibel sind, gibt es zwei Möglichkeiten:

- Installieren Sie die Sicherheitsagenten einschließlich dem Verschlüsselungsmodul.
- Verwenden Sie die Aufgabe **Neu konfigurieren**.

Weitere Informationen zur Verwendung von Full Disk Encryption in Ihrem Netzwerk finden Sie im Kapitel **Sicherheitsrichtlinien > Verschlüsselung** im GravityZone-Administratorhandbuch.

5.5. Schutz für Exchange installieren

Security for Exchange integriert sich automatisch mit den Excchange-Servern je nach Server-Rolle. Für jede Rolle werden entsprechend der folgenden Übersicht nur die kompatiblen Funktionen installiert:

Bestandteile	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Postfach	Edge	Hub	Postfach
Transport-Ebene					
Malware-Filter	x	x	x	x	
Antispam-Filterung	x	x	x	x	
Inhaltsfilterung	x	x	x	x	
Anhangsfilterung	x	x	x	x	
Exchange-Informationsspeicher					
Bedarf-Malware-Scans		x			x

5.5.1. Vor der Installation

Bevor Sie Security for Exchange installieren, sollten Sie sich vergewissern, dass alle Voraussetzungen erfüllt sind, da sonst eventuell Bitdefender Endpoint Security Tools ohne das Exchange-Schutz-Modul installiert wird.

Damit das Exchange-Schutz-Modul möglichst reibungslos läuft und etwaige Konflikte und unerwünschte Ergebnisse vermieden werden, sollten Sie andere Malware-Schutz- und E-Mail-Filter-Agenten deinstallieren.

Bitdefender Endpoint Security Tools findet und entfernt die meisten Virenschutzprodukte automatisch und deaktiviert auch den Malware-Schutz-Agenten, der seit Version 2013 in Exchange Server enthalten ist. Eine Liste aller automatisch gefundenen und entfernten Sicherheitssoftware finden Sie in diesem Artikel.

Den eingebauten Exchange-Malware-Schutz-Agenten können Sie jederzeit manuell wieder aktivieren. Dies wird jedoch nicht empfohlen.

5.5.2. Schutz auf Exchange-Servern installieren

Um Ihre Exchange-Server zu schützen, müssen Sie Bitdefender Endpoint Security Tools mit der Exchange-Schutz-Rolle auf jedem dieser Server installieren.

Dazu haben Sie verschiedene Möglichkeiten:

- Lokale Installation durch Herunterladen und Ausführen des Installationspakets auf dem jeweiligen Server.

- Ferninstallation durch Ausführen der Aufgabe **Installieren**.
- Per Fernzugriff durch Ausführen der Aufgabe **Client neu konfigurieren**, falls Bitdefender Endpoint Security Tools bereits das Dateisystem auf dem Server schützt.

Weitere Details zur Installation finden Sie unter „Sicherheitsagent installieren“ (S. 41).

5.6. Speicherschutz installieren

Security for Storage ist ein Bitdefender-Dienst zum Schutz von NAS-Geräten (Network-attached Storage) und Filesharing-Systemen, die das Internet Content Adaptation Protocol (ICAP) unterstützen. Informationen zu unterstützten Filesharing-Systemen finden Sie unter „Speicherschutz“ (S. 35).

So verwenden Sie Security for Storage in Kombination mit Ihrer GravityZone-Lösung:

1. Installieren und konfigurieren Sie mindestens zwei Security Server in Ihrer Umgebung als ICAP-Server. Bitdefender Security Server analysieren Dateien, senden Ergebnisse an Speichersysteme und führen bei Bedarf entsprechende Aktionen durch. Bei Überlastung leitet der erste Security Server die übrigen Daten an den zweiten weiter.

   Beachten Sie
   Wir empfehlen, Security Server, die dem Speicherschutz dienen, getrennt von Security Servern zu installieren, die für andere Rollen wie Malware-Scans eingesetzt werden.

   Details zur Installation von Security Servern finden Sie in diesem Handbuch unter **Security Server installieren**.

2. Konfigurieren Sie das Modul **Speicherschutz** über die GravityZone-Richtlinieneinstellungen.

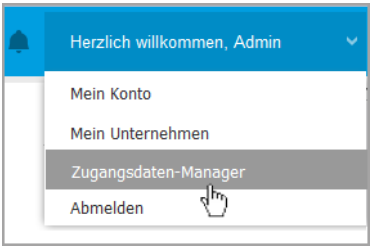
   Nähere Informationen finden Sie unter **Sicherheitsrichtlinien > Richtlinien für Computer und virtuelle Maschinen > Speicherschutz** im GravityZone-Administratorhandbuch.

Details zur Konfiguration und Verwaltung von ICAP-Servern auf bestimmten NAS-Geräten oder Filesharing-Systemen entnehmen Sie bitte der Dokumentation der entsprechenden Plattform.

5.7. 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**.

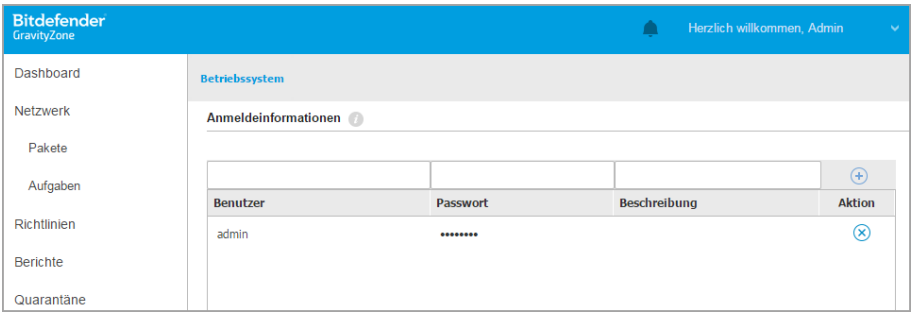


Das Zugangsdaten-Manager-Menü

5.7.1. 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.

5.7.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen

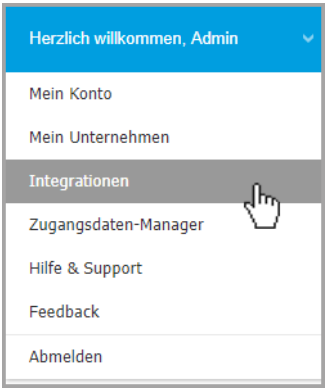
So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

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.

6. INTEGRATIONEN

Mithilfe von GravityZone kann das Control Center mit Drittanbieterlösungen integriert werden.

Die Integration Ihrer Drittanbieter-Lösungen können Sie auf der Seite **Integrationen** konfigurieren. Sie gelangen zu dieser Seite, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren und dann **Integrationen** wählen.



Auf dieser Seite können Sie nach Bedarf Integrationen hinzufügen, bearbeiten und entfernen.

6.1. Integration mit Microsoft Windows Defender ATP

Durch die Integration zwischen GravityZone und der Windows Defender Advanced Threat Protection können Microsoft-Kunden die Sicherheit ihrer macOS- und Linux-Endpunkte innerhalb der Oberfläche des Windows-Defender-Sicherheitscenters verwalten.

Mit dieser Integration sendet GravityZone Informationen über Malware und über den Produktstatus von den verwalteten macOS- und Linux-Endpunkten an das Windows Defender Security Center.

Befolgen Sie die in diesem Artikel in der Wissensdatenbank beschriebenen Anweisungen, um GravityZone mit Microsoft Windows Defender ATP zu integrieren.

7. SCHUTZ DEINSTALLIEREN

Sie können GravityZone-Komponenten deinstallieren und neu installieren, wenn Sie zum Beispiel einen Lizenzschlüssel für eine andere Maschine benötigen, um Fehler zu beheben oder ein Upgrade zu installieren.

Um den Bitdefender-Schutz von den Endpunkten in Ihrem Netzwerk ordnungsgemäß zu entfernen, folgen Sie bitte den Anweisungen in diesem Kapitel.

- Endpunkt-Schutz deinstallieren
- Exchange-Schutz deinstallieren

7.1. Endpunkt-Schutz deinstallieren

Um den Bitdefender-Schutz sicher zu entfernen, müssen Sie zuerst die Sicherheitsagenten und dann, falls nötig, den Security Server deinstallieren. Wenn Sie nur den Security Server deinstallieren wollen, stellen Sie sicher, dass sein Agent zuerst mit einem anderen Security Server verbunden ist.

- Sicherheitsagenten deinstallieren
- Security Server deinstallieren

7.1.1. Sicherheitsagenten deinstallieren

Die Sicherheitsagenten können auf zwei Arten deinstalliert werden:

- Per Fernzugriff über Control Center
- Manuell auf der Zielmaschine

Fern-Deinstallation

So deinstallieren Sie den Bitdefender-Schutz per Fernzugriff von jedem beliebigen verwalteten Endpunkt aus:

1. Öffnen Sie die Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Computer des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Wählen Sie die Endpunkte aus, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.

4. Klicken Sie auf **Aufgaben** oben in der Tabelle und wählen Sie dann **Client deinstallieren**. Ein Konfigurationsfenster wird geöffnet.
5. Im Fenster **Agent deinstallieren** können Sie auswählen, ob Sie in Quarantäne befindliche Dateien an den Endpunkten behalten oder löschen wollen.
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.

Lokale Deinstallation

So deinstallieren Sie den Sicherheitsagenten von Bitdefender auf einer Windows-Maschine:

1. Abhängig von Ihrem Betriebssystem:
   - Bei Windows 7 öffnen Sie **Start > Systemsteuerung > Programm deinstallieren** im Abschnitt **Programme**.
   - Bei Windows 8 öffnen Sie **Einstellungen > Systemsteuerung > Programm deinstallieren** im Abschnitt **Programme**.
   - Bei Windows 8.1 klicken Sie mit der rechten Maustaste **Start** und wählen Sie dann **Systemsteuerung > Programme & Funktionen**.
   - Bei Windows 10 öffnen Sie **Start > Einstellungen > System > Apps & Funktionen**.
2. Wählen Sie in der Programmliste den Bitdefender-Agenten.
3. Klicken Sie auf **Deinstallieren**.
4. Geben Sie das Bitdefender-Passwort ein, falls es in den Sicherheitsrichtlinien aktiviert ist. Während der Deinstallation können Sie den Prozessfortschritt anzeigen.

So deinstallieren Sie den Bitdefender-Sicherheitsagenten manuell von einer Linux-Maschine:

1. Terminal öffnen.
2. Root-Zugang erhalten Sie über den Befehl `su` oder `sudo su`.
3. Öffnen Sie mit dem Befehl `cd` den folgenden Pfad: `/opt/BitDefender/bin`
4. Führen Sie folgendes Script aus:

```
# ./remove-sve-client
```

5. Zum Fortfahren geben Sie das Bitdefender-Passwort ein, sofern dies in den Sicherheitsrichtlinien aktiviert ist.

So deinstallieren Sie den Bitdefender-Agenten von einem Mac:

1. Öffnen Sie **Finder > Anwendungen**.
2. Öffnen Sie den Bitdefender-Ordner.
3. Doppelklicken Sie **Bitdefender Mac deinstallieren**.
4. Klicken Sie im Bestätigungsfenster **Überprüfen** und **Deinstallieren**.

7.1.2. Security Server deinstallieren

So entfernen Sie den Security Server:

1. Schalten Sie die virtuelle Maschine des Security Server aus und entfernen Sie sie aus Ihrer virtuellen Umgebung.
2. Melden Sie sich am GravityZone Control Center an.
3. Im Bereich **Netzwerk** finden Sie im Inventar den Security Server. Wenn Sie die virtuelle Maschine gelöscht haben, wird der Security Server nach einer Weile als offline angezeigt.
4. Markieren Sie das Kästchen des Security Server.
5. Klicken Sie in der Symbolleiste auf die Schaltfläche ⊖ **Löschen**.

   Der Security Server wird in den Ordner **Gelöscht** verschoben. Von dort aus können Sie ihn vollständig entfernen, indem Sie noch einmal in der Symbolleiste auf die Schaltfläche ⊖ **Löschen** klicken.

7.2. Exchange-Schutz deinstallieren

Sie können den Exchange-Schutz von jedem Microsoft-Exchange-Server entfernen, wenn für diese Rolle Bitdefender Endpoint Security Tools installiert ist. Sie können die Deinstallation auch über Control Center vornehmen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Die Entitäten werden im rechten Fenster angezeigt.

3. Wählen Sie den Endpunkt, von dem der Exchange-Schutz deinstalliert werden soll.
4. Klicken Sie **Client neu konfigurieren** im **Aufgaben**- Menü im oberen Teil der Tabelle an. Ein Konfigurationsfenster wird geöffnet.
5. Entfernen Sie im Bereich **Allgemein** das Häkchen im Kästchen **Exchange-Schutz**.

   Warnung
   Stellen Sie über das Konfigurationsfenster sicher, dass alle anderen am Endpunkt aktiven Rollen ausgewählt sind. Andernfalls werden diese ebenfalls deinstalliert.

6. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen.

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

Unter „Schutz für Exchange installieren“ (S. 67) können Sie den Exchange-Schutz neu installieren.

8. 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.

8.1. 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.

8.2. Hilfe anfordern

Nutzen Sie unser Online-Support-Center, um Unterstützung anzufordern. Füllen Sie das Kontaktformular aus und senden Sie es ab.

8.3. 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.

8.3.1. 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.

8.3.2. 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

8.3.3. 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.

8.4. 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.

8.4.1. 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

8.4.2. 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.

8.4.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

USA

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (Vertrieb&Technischer Support): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/support/business.html

Frankreich

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-Mail: b2b@bitdefender.fr
Website: http://www.bitdefender.fr
Support-Center: http://www.bitdefender.fr/support/business.html

Spanien

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15
Telefon (Technischer Support): (+34) 93 502 69 10
Vertrieb: comercial@bitdefender.es
Website: http://www.bitdefender.es
Support-Center: http://www.bitdefender.es/support/business.html

Deutschland

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (Geschäftsstelle&Vertrieb): +49 (0) 2304 94 51 60
Telefon (Technischer Support): +49 (0) 2304 99 93 004
Vertrieb: firmenkunden@bitdefender.de
Website: http://www.bitdefender.de
Support-Center: http://www.bitdefender.de/support/business.html

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire

ST6 4BF
UK
Telefon (Vertrieb&Technischer Support): (+44) 203 695 3415
E-Mail: info@bitdefender.co.uk
Vertrieb: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support-Center: http://www.bitdefender.co.uk/support/business.html

Rumänien

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (Vertrieb&Technischer Support): +40 21 2063470
Vertrieb: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Support-Center: http://www.bitdefender.ro/support/business.html

Vereinigte Arabische Emirate

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (Vertrieb&Technischer Support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/support/business.html

A. Anhänge

A.1. Unterstützte Dateitypen

Die Malware-Scan-Engines der Bitdefender-Sicherheitslösungen können sämtliche Dateitypen scannen, in denen Bedrohungen versteckt sein könnten. Die folgende Liste zeigt die am häufigsten gescannten Dateitypen.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

A.2. Sandbox Analyzer-Objekte

A.2.1. 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.2.2. 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.2.3. Standardausschlüsse bei automatischer Übermittlung

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

A.3. Vom Vorfallsensor unterstützte Kernel

Der Vorfallsensor unterstützt die folgenden Kernel: