Bitdefender

GravityZone

HANDBUCH FÜR SICHERHEITSANALYSTEN

Bitdefender GravityZone
Handbuch für Sicherheitsanalysten

Veröffentlicht 2021.01.12

Rechtlicher Hinweis

Inhaltsverzeichnis

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)**

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. 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.

3.2. 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

3.2.1. 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.

Schutzebenen

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

- Malware-Schutz
- Advanced Threat Control
- HyperDetect
- Firewall

- Inhalts-Steuerung
- Network Attack Defense
- Patch-Verwaltung
- Gerätesteuerung
- Full Disk Encryption
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpunkt-Risikoanalyse (ERA)

Endpunktrollen

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

Power-User

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

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

Relais

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

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

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

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

-
- 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.

3.2.2. 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

3.3. Sandbox Analyzer-Architektur

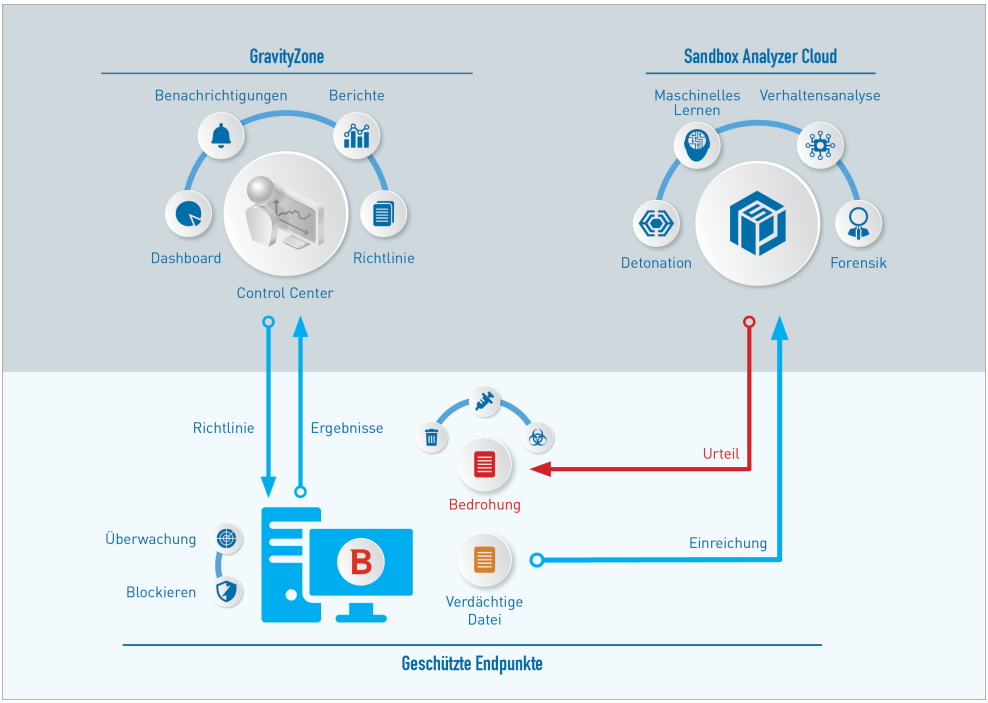
Der Bitdefender Sandbox Analyzer bietet hohe Sicherheit vor raffinierten Bedrohungen, indem automatische, detaillierte Analysen verdächtiger Dateien durchgeführt werden; selbst solcher Dateien, die noch keine Signatur von den Bitdefender-Malware-Schutz-Engines erhalten haben.

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.

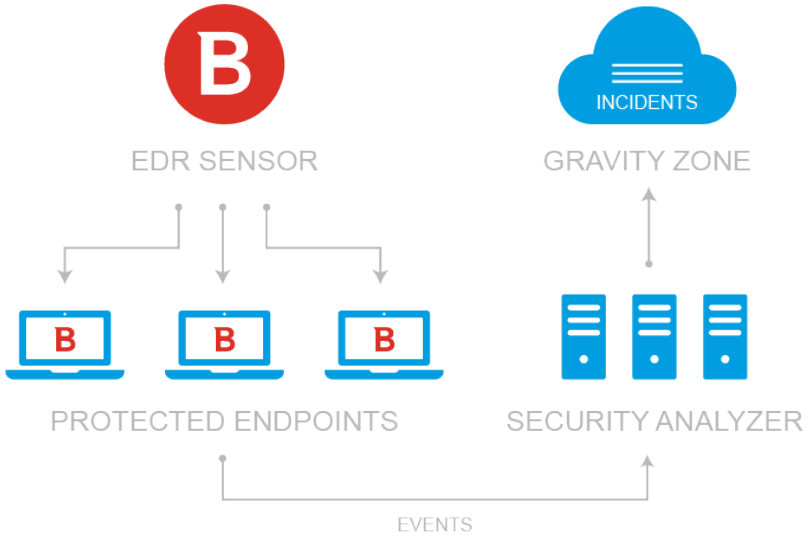
Die Analyseergebnisse werden mit ihrem Datei-Hash-Wert in der Sandbox Analyzer-Datenbank gespeichert. Wenn eine bereits zuvor analysierte Datei von einem anderen Endpunkt gemeldet wird, wird sofort eine Antwort zurückgegeben, da die Ergebnisse bereits in der Datenbank vorhanden sind.

3.4. EDR-Architektur

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

EDR umfasst zwei Hauptkomponenten:

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



EDR im Zusammenhang mit Datenfluss vom Endpunkt zum Control Center

4. ERSTE SCHRITTE

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

4.1. Verbinden mit dem Control Center

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

Vorbereitende Maßnahmen:

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

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

So stellen Sie eine Verbindung zum Control Center her:

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

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

Sie werden dann von GravityZone zur Authentisierungsseite Ihres Identitätsanbieters weitergeleitet.

b. Authentisieren Sie sich bei Ihrem Identitätsanbieter.

c. Vom Identitätsanbieter werden Sie dann zurück zu GravityZone geleitet, wo Sie automatisch am Control Center angemeldet werden.

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

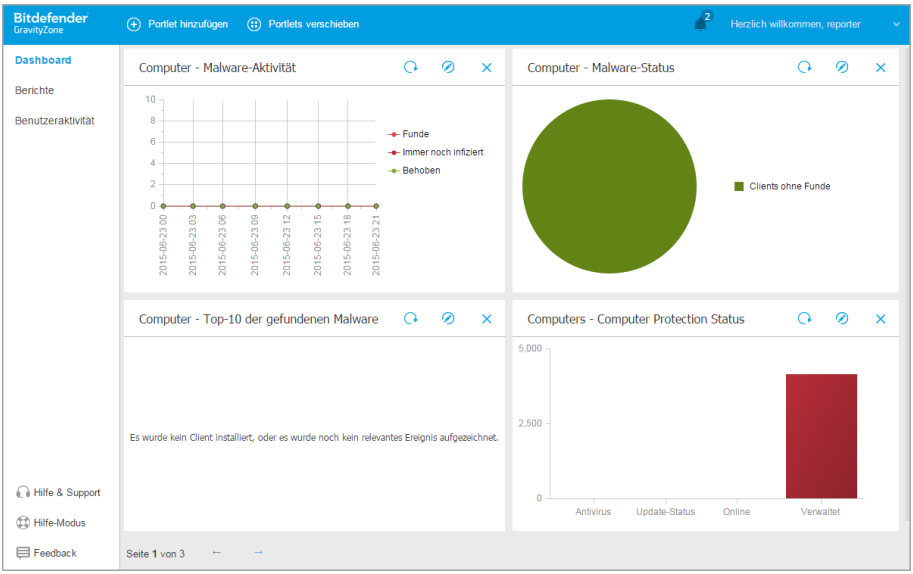
Bei der ersten Anmeldung müssen Sie den Bitdefender-Nutzungsbedingungen zustimmen. Mit einem Klick auf **Fortfahren** können Sie mit der Nutzung von GravityZone loslegen.

Beachten Sie

- Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern. Sie müssen die E-Mail-Adresse Ihres Kontos angeben.
- Sollte Sie GravityZone bei der Anmeldung mit SSO nach einem Passwort fragen, wenden Sie sich bitte an Ihren Administrator. In der Zwischenzeit können Sie sich mit Ihrem vorigen Passwort anmelden oder über den Link zur Passwortwiederherstellung ein neues Passwort anfordern.

4.2. Control Center auf einen Blick

Control Center ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten. Verwenden Sie die Menüleiste im oberen Bereich, um durch die Konsole zu navigieren.



Das Dashboard

Sicherheitsanalysten können über die Menüleiste auf die folgenden Bereiche zugreifen:

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

Berichte
Sicherheitsberichte über verwaltete Clients erhalten.

Benutzeraktivität
Das Benutzeraktivitätsprotokoll einsehen.

Wenn Sie den Mauszeiger über den Benutzernamen in der rechten oberen Ecke der Konsole bewegen, erhalten Sie die folgenden Optionen:

- **Mein Konto**. Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Hilfe & Support**. Klicken Sie auf diese Option, um Hilfe- und Support-Informationen zu erhalten.

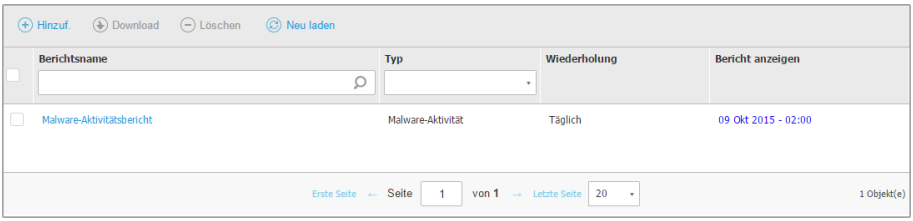
- **Feedback**. Klicken Sie auf diese Option, um ein Formular zu öffnen, über das Sie uns Rückmeldung zu Ihren Erfahrungen mit GravityZone geben können.
- **Abmelden**. Klicken Sie auf diese Option, um sich bei Ihrem Konto abzumelden.

Rechts oben in der Konsole finden Sie außerdem:

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

4.2.1. Tabellendaten

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



Die Berichteseite

Durch Tabellenseiten blättern

Tabellen mit mehr als 20 Einträgen haben mehr als eine Seite. Standardmäßig werden nur 20 Einträge pro Seite angezeigt. Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Sie können die Anzahl der Einträge, die pro Seite angezeigt werden, ändern, indem Sie eine andere Option aus dem Menü neben den Navigationsschaltflächen wählen.

Nach bestimmten Einträgen suchen

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

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

Daten sortieren

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

Tabellendaten neu laden

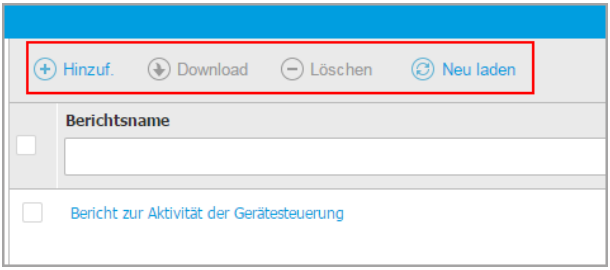
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**.

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

4.2.2. Symbolleisten

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

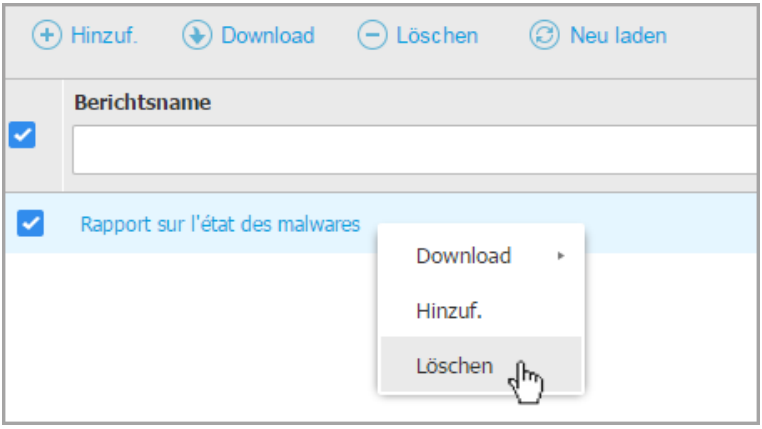
- Neuen Bericht erstellen.
- Einen geplanten Bericht herunterladen.
- Einen geplanten Bericht löschen.



Die Berichteseite - Symbolleiste

4.2.3. Kontextmenü

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



Die Berichteseite - Kontextmenü

4.3. Ändere Login Passwort

Nachdem Ihr Konto angelegt wurde, erhalten Sie eine E-Mail mit den Anmeldedaten.

Es empfiehlt sich, wie folgt vorzugehen:

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

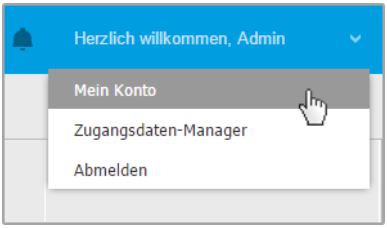
Um das Anmeldepasswort zu ändern:

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

4.4. Verwalten Ihres Kontos

So überprüfen oder ändern Sie Ihre Kontodetails und -Einstellungen:

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



Das Benutzerkontomenü

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

   So aktivieren Sie die Zwei-Faktor-Authentifizierung:

   a. **Zwei-Faktor-Authentifzierung.** Die Zwei-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsschicht für Ihr GravityZone-Konto, da sie erfordert,

dass Sie bei der Anmeldung an Ihrem Konto außer den Zugangsdaten für das Control Center noch einen Authentifizierungscode eingeben.

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

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

So aktivieren Sie die Zwei-Faktor-Authentifizierung:

i. Klicken Sie unter der Meldung **Zwei-Faktor-Authentifizierung** auf **Aktivieren**.

ii. Klicken Sie im Dialogfeld auf den entsprechenden Link, um Google Authenticator herunterzuladen und auf Ihrem Mobilgerät zu installieren.

iii. Öffnen Sie Google Authenticator auf Ihrem Mobilgerät.

iv. Scannen Sie im Bildschirm **Konto hinzufügen** den QR-Code, um die App mit Ihrem GravityZone-Konto zu verknüpfen.

Sie können auch den geheimen Schlüssel manuell eingeben.

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

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

Schlüssel eingeben, um das neue Gerät mit Ihrem GravityZone-Konto zu verknüpfen.

v. Geben Sie den sechsstelligen Code in das Feld **Google-Authenticator-Code** ein.

vi. Klicken Sie auf **Aktivieren**, um die Funktion zu aktivieren.

Beachten Sie
Ihr Unternehmensadministrator kann die Zwei-Faktor-Authentifizierung für alle GravityZone-Benutzerkonten zwingend erforderlich machen. Ist dies der Fall, werden Sie bei der Anmeldung aufgefordert, Ihre 2FA zu konfigurieren. Sie können die Zwei-Faktor-Authentifizierung (2FA) für Ihr Benutzerkonto zudem nicht deaktivieren, solange diese Funktion durch Ihren Unternehmensadministrator zwingend vorgeschrieben ist.
Bitte beachten Sie, dass dieser geheime Schlüssel seine Gültigkeit verliert, wenn die aktuell konfigurierte 2FA für Ihr Benutzerkonto deaktiviert wird,

b. **Passwortablaufrichtlinie.** Durch regelmäßige Änderung Ihres Passworts erhalten Sie zusätzlichen Schutz vor nicht autorisierter Verwendung von Passwörtern oder begrenzen die Dauer von nicht autorisierter Verwendung. Wenn diese Richtlinie aktiviert ist, müssen Sie Ihr GravityZone-Passwort spätestens alle 90 Tage ändern.

c. **Kontosperrungsrichtlinie.** Diese Richtlinie verhindert den Zugriff auf Ihr Konto nach fünf aufeinander folgenden fehlgeschlagenen Anmeldeversuchen. Diese Maßnahme dient dem Schutz vor Brute-Force-Angriffen.

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

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

Beachten Sie
Sie können Ihr eigenes Konto nicht löschen.

5. ÜBERWACHUNGS-DASHBOARD

Die ordnungsgemäße Analyse Ihrer Netzwerksicherheit erfordert Datenzugriff und -korrelation. Zentral verfügbare Sicherheitsinformationen ermöglichen es Ihnen, die Einhaltung der Sicherheitsrichtlinien des Unternehmens zu überwachen und sicherzustellen, Probleme schnell zu identifizieren und Bedrohungen und Schwachstellen zu analysieren.

5.1. Dashboard

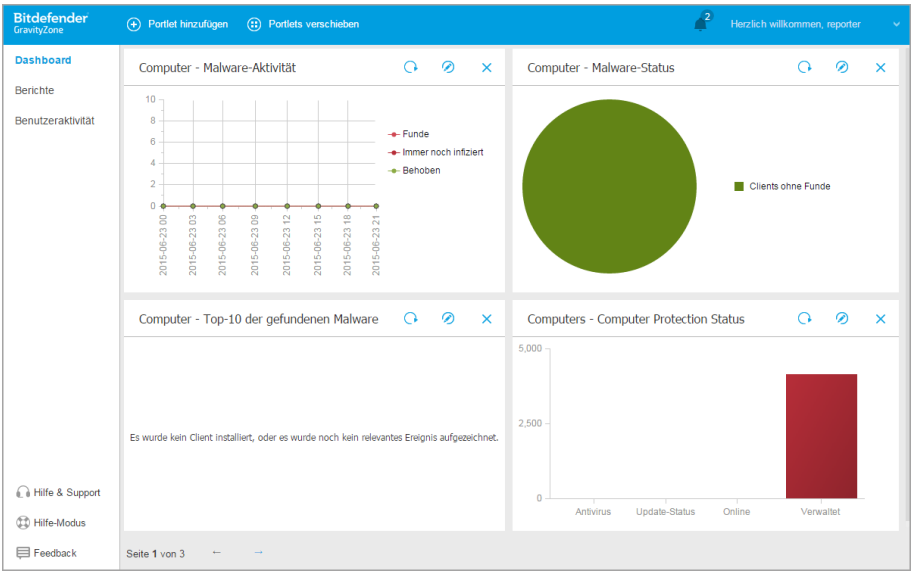
Das Control Center-Dashboard ist eine individuell anpassbare Oberfläche, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Endpunkte und den Netzwerkstatus verschafft.

Es besteht aus zwei Bereichen:

- Dashboard-Netzwerkstatusleiste
- Dashboard-Portlets

Die Dashboard-Netzwerkstatusleiste hält Sie über die Anzahl der offenen oder laufenden Vorfälle, bedrohten Assets (Endpunkte) und erkannte Bedrohungen in Ihrem Netzwerk auf dem Laufenden. Nutzen Sie diese Informationen, um nicht behobene Netzwerkobjekte zu überfliegen. Klicken Sie auf **Ansicht**, um die Seite **Vorfälle** aufzurufen. Weitere Informationen finden Sie unter „Vorfälle untersuchen“ (S. 29).

In den Dashboard-Portlets werden verschiedenste Echtzeit-Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie bieten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.



Das Dashboard

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center verfügt über verschiedene vordefinierte Dashboard-Portlets.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Es gibt eine Reihe verschiedener Portlet-Typen, die unterschiedliche Informationen über den Schutz Ihrer Endpunkte enthalten, so zum Beispiel Update-Status, Malware-Status, Firewall-Aktivität.

  Beachten Sie
  Standardmäßig rufen die Portlets Daten für den heutigen Tag ab. Im Gegensatz zu Berichten können sie nicht auf Intervalle eingestellt werden, die länger als ein Monat sind.

- Die in den Portlets angezeigten Informationen beziehen sich nur auf Endpunkte unter Ihrem Konto. Sie können die Ziele und Präferenzen jedes Portlets mit dem Befehl **Portlet bearbeiten** an Ihre Bedürfnisse anpassen.

- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Die Portlets werden in Vierergruppen angezeigt. Mit der senkrechten Scroll-Leiste oder den Pfeiltasten können Sie von einer Portlet-Gruppe zur nächsten navigieren.
- Bei verschiedenen Berichttypen haben Sie die Möglichkeit, sofort bestimmte Aufgaben auf den Zielendpunkten ausführen zu lassen, ohne dazu erst auf die Seite **Netzwerk** wechseln zu müssen; so können Sie z. B. infizierte Endpunkte scannen oder Endpunkte aktualisieren. Über die Schaltfläche am unteren Rand des Portlets können Sie die entsprechende Aktion ausführen.

Das Dashboard lässt sich nach individuellen Vorlieben leicht konfigurieren. Sie können Portlet-Einstellungen bearbeiten, neue Portlets hinzufügen, Portlets entfernen oder die bestehenden Portlets neu anordnen.

5.1.1. Portlet-Daten neu laden

Um sicherzustellen, dass das Portlet die aktuellsten Informationen anzeigt, klicken Sie auf die Schaltfläche **Neu laden** in der entsprechenden Titelleiste.

Um die Daten in allen Portlets gleichzeitig zu aktualisieren, klicken Sie oben im Dashboard auf die Schaltfläche **Portlets aktualisieren**.

5.1.2. Portlet-Einstellungen bearbeiten

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an. Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die das Symbol **Portlet bearbeiten** in der entsprechenden Titelleiste klicken.

5.1.3. Ein neues Portlet hinzufügen

Sie können andere Portlets hinzufügen, um bestimmte Informationen angezeigt zu bekommen.

So fügen Sie ein neues Portlet hinzu:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlet hinzufügen** am oberen Rand der Konsole. Das Konfigurationsfenster wird geöffnet.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:

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

Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter „Berichtstypen“ (S. 104).

4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die Sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

5.1.4. Ein Portlet entfernen

Sie können ein Portlet ganz einfach entfernen, indem Sie in seiner Titelleiste auf das Symbol ⊗ **Entfernen** klicken. Wenn Sie ein Portlet einmal entfernt haben, können Sie es nicht wiederherstellen. Sie können aber ein neues Portlet mit genau denselben Einstellungen erstellen.

5.1.5. Portlets neu anordnen

Sie können die Portlets im Dashboard ganz nach Ihren Bedürfnissen anordnen. So ordnen Sie die Portlets neu an:

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

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

6. VORFÄLLE UNTERSUCHEN

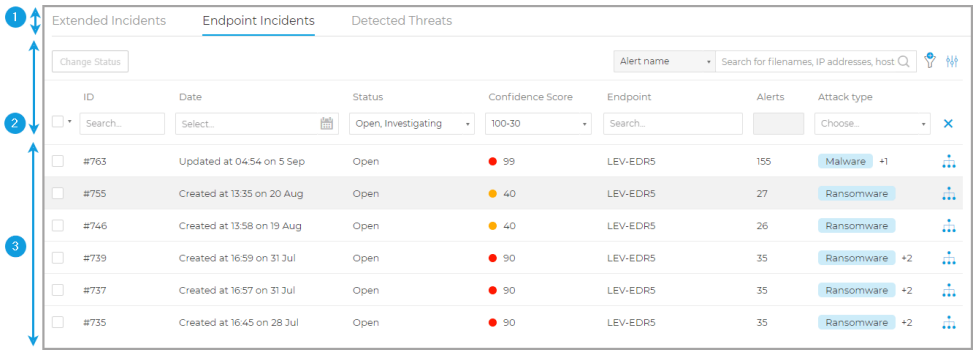
Im Bereich **Vorfälle** können Sie alle vom Vorfall-Sensor während eines bestimmten Zeitraums gemeldeten Sicherheitsereignisse untersuchen, filtern und entsprechende Bereinigungsaktionen durchführen.

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

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

6.1. Die Vorfallsseite

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



Vorfallsübersicht

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

Diese Seite umfasst die folgenden Bereiche:

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

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

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

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

Beachten Sie
Diese Funktion unterstützt nicht mehr den Internet Explorer.

Die Übersichtsleiste

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

Die Übersichtsleiste

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

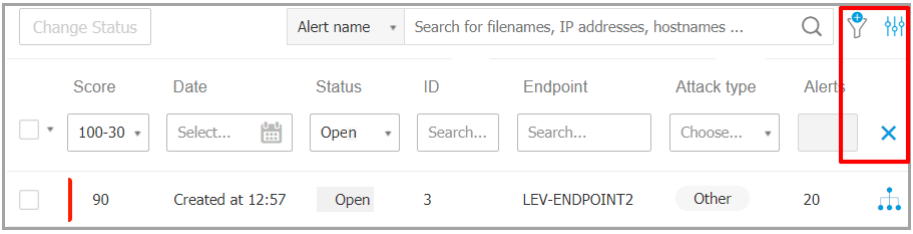
Vorfälle in der Übersichtsleiste filtern

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

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

6.1.1. Die Filterleiste

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



Die Filterleiste

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

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

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

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

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

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

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

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

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

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

6.1.2. Liste der Sicherheitsereignisse anzeigen

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

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

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

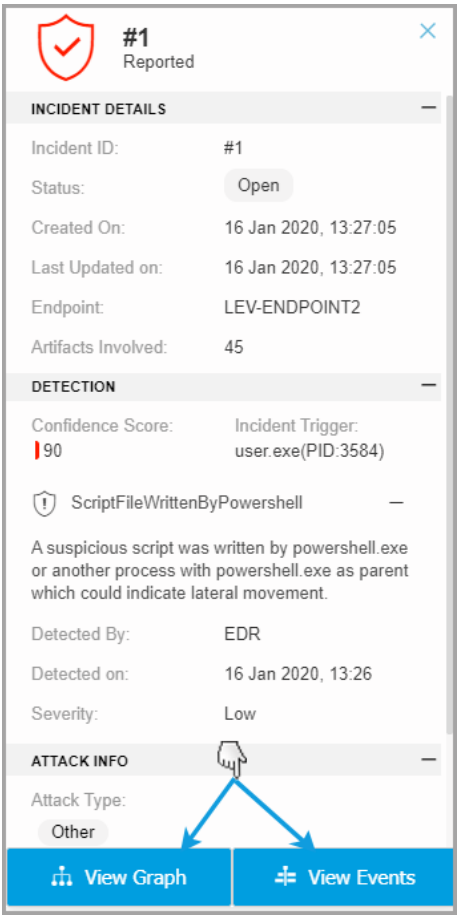
Die Seite hoch und runter scrollen können Sie mithilfe der Pfeiltasten, des Mausrads oder der Scroll-Leiste. Sie können unten auf der Seite die Anzahl der angezeigten Ereignisse anpassen. Sie können bis zu 100 Ereignisse pro Seite anzeigen.

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

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

Sicherheitsereigniskarte

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



Schnellansicht der Details zu einem Vorfall

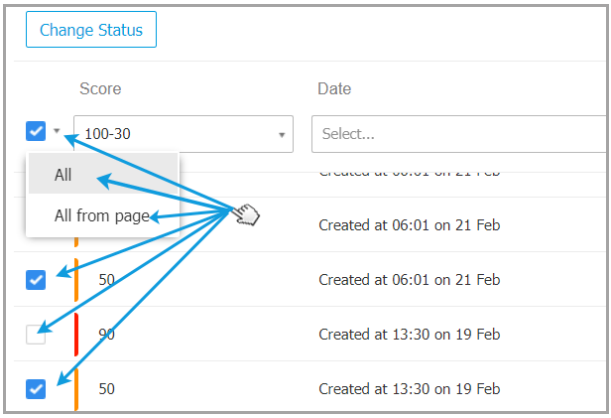
  - Wenn Sie hier auf die Schaltfläche **Diagramm anzeigen** klicken, wird eine graphische Darstellung des Vorfalls angezeigt.
  - Wenn Sie auf die Schaltfläche **Ereignisse anzeigen** klicken, wird die Zeitleiste des Vorfalls angezeigt.
- Wenn Sie das Kästchen einer Sicherheitsereigniskarte markieren, wird die Schaltfläche **Status ändern** aktiviert, über die Sie den Status des Vorfalls ändern können.

Ändern des Status von Sicherheitsereignissen

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

Sie können den Status eines oder mehrerer Sicherheitsereignisse gleichzeitig ändern:

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

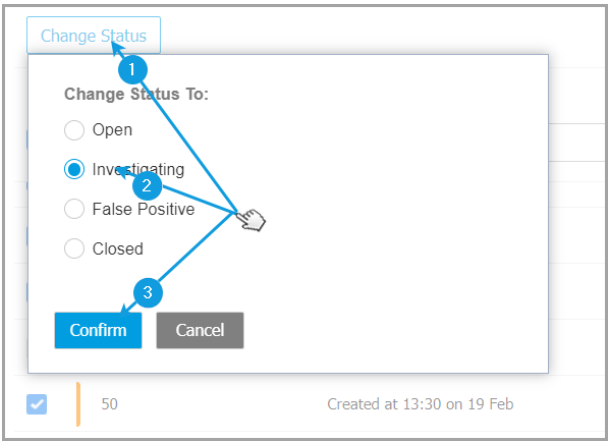


Sicherheitsereigniskarten markieren

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

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

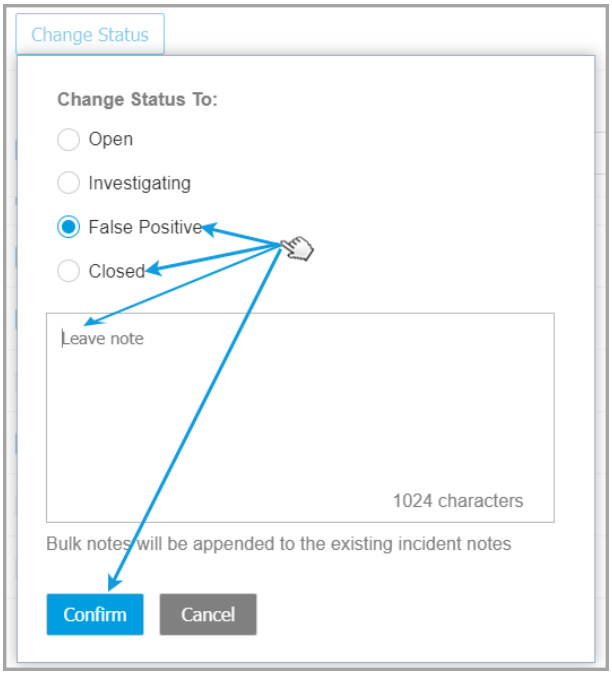
2. Klicken Sie auf die Schaltfläche **Status ändern** und wählen Sie die gewünschte Option:



Ändern des Status von Sicherheitsereignissen

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

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



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

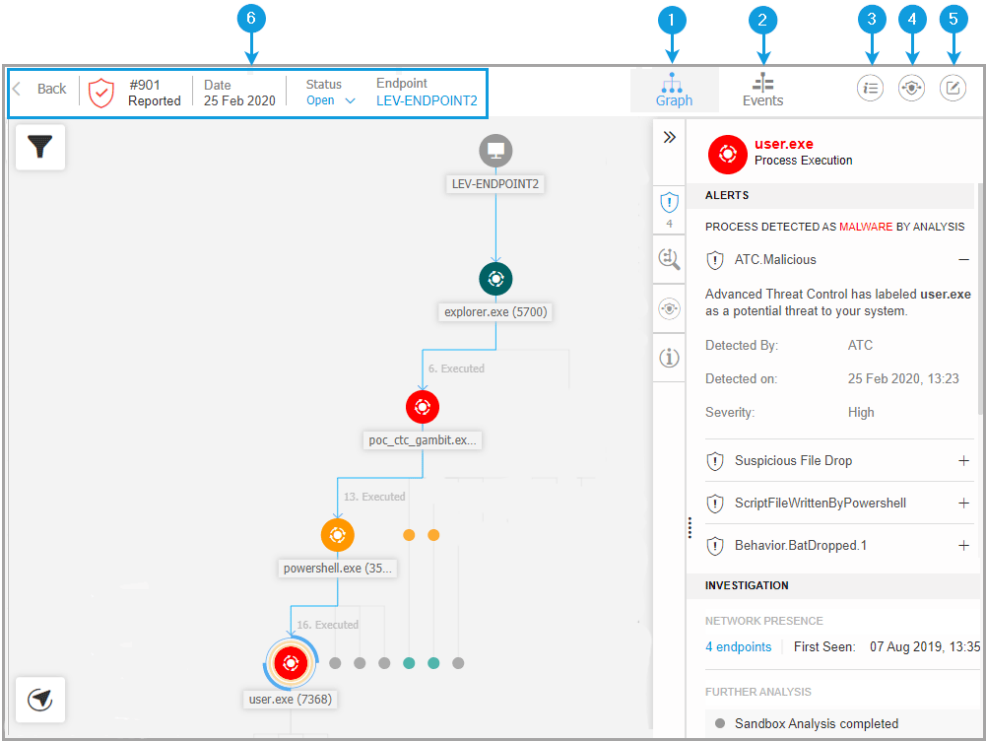
Beachten Sie
Die Notiz wird zu evtl. schon bestehenden hinzugefügt.

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

6.1.3. Untersuchen eines Endpunktvorfalls

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

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


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

1. Diagrammreiter

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

2. Ereignisreiter

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

3. Vorfallsinformationen

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

4. Bereinigung

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

5. Zwischenablage für Notizen

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

6. Vorfallstatusleiste

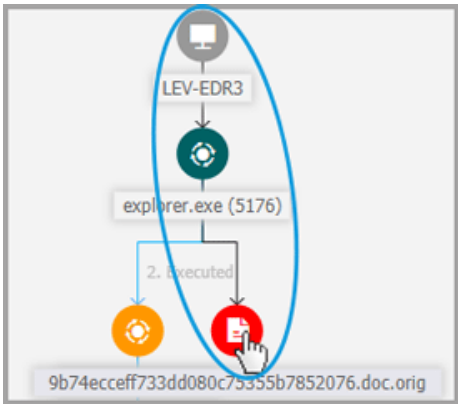
   Die Statusleiste zeigt Details zur ID des Vorfalls, zu Uhrzeit und Datum der Erstellung, zum Status, zum Auslöser des Vorfalls und zum Endpunkt, den er beeinträchtigt. Mit einem Klick auf die Schaltfläche **Zurück** gelangen Sie zurück zur Hauptseite **Vorfälle**.

Sicherheitsereignisknoten

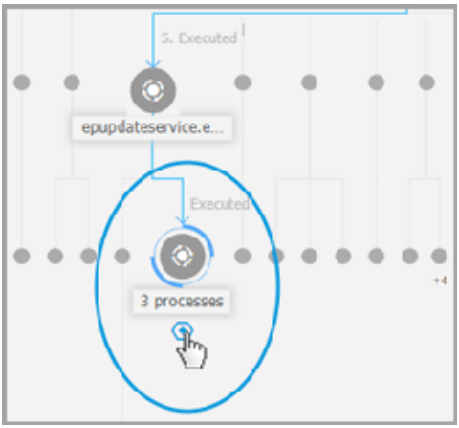
Wissenswertes zu den Sicherheitsereignisknoten:

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

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



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



  - Nur Knoten ohne untergeordnete Elemente werden beim Reduzieren des Clusterknotens aus dem Ereignisdiagramm ausgeblendet.
  - Knoten, bei denen verdächtige Aktivitäten erkannt wurden, werden dem Clusterknoten nicht hinzugefügt.
- Mit einem Klick auf einen Knoten können Sie die folgenden Details anzeigen:
  - Der Pfad zum Endpunktknoten und alle beteiligten Elemente werden in Blau hervorgehoben.
  - Eine Seitenleiste mit erweiterbaren Abschnitten, die Details zu ausgewählten Knoten, Warnmeldungen zu Funden, verfügbare Aktionen und Empfehlungen anzeigen. Unter „Knotendetails“ (S. 55) finden Sie weitere Informationen.
- Die Knoten sind durch Pfeillinien verbunden, die den Verlauf der Aktionen anzeigen, die während des Vorfalls auf dem Endpunkt stattgefunden haben. Jede Linie ist mit dem Aktionsnamen und einer chronologischen Nummerierung versehen.

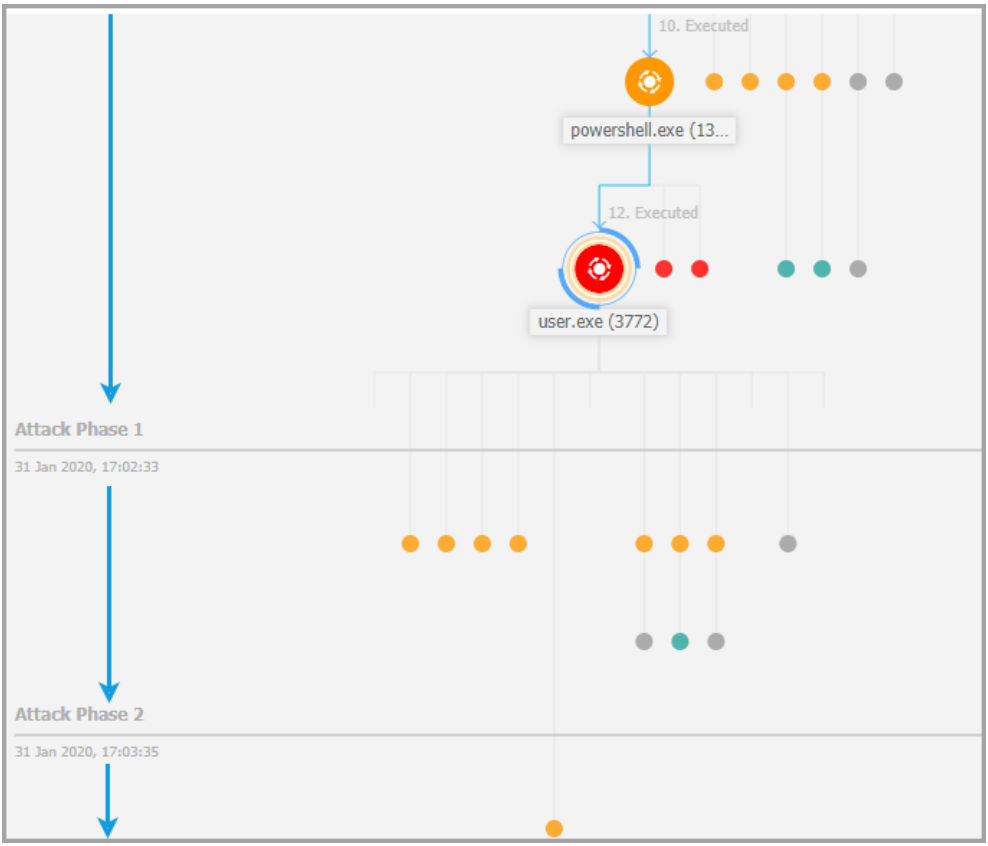
Die folgenden Elemente eines Vorfalls können als Knoten dargestellt werden:

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

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

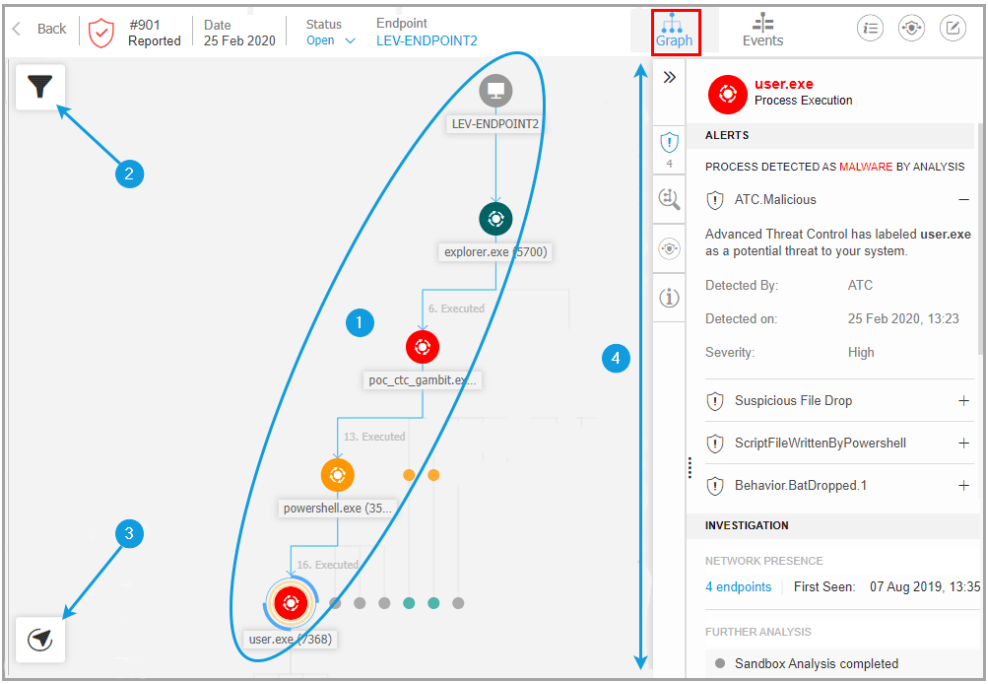
Diagramm

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



Mehrstufiger Angriff

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



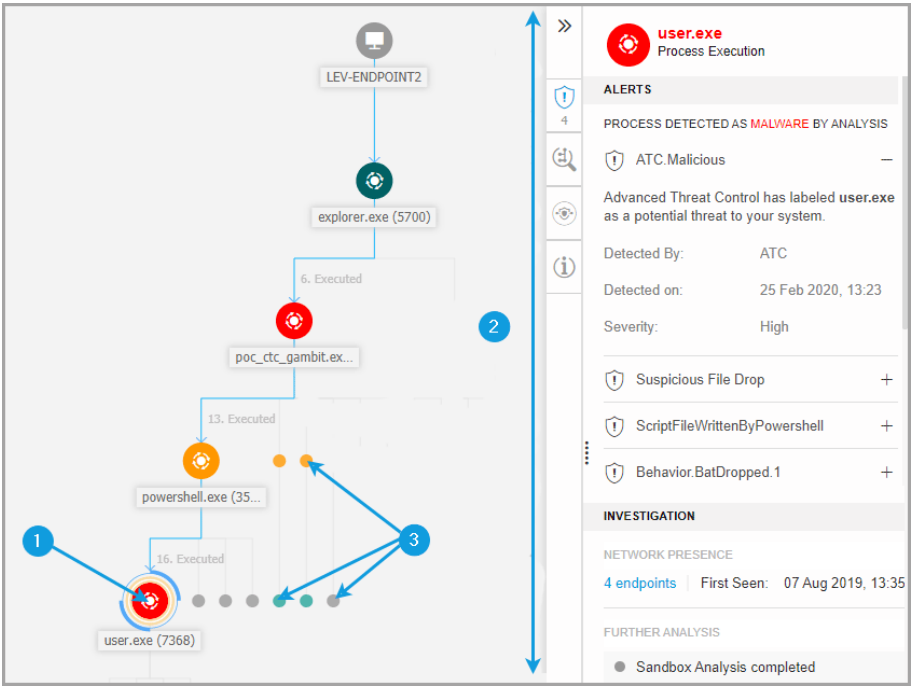
Diagrammreiter

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

Kritischer Pfad

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

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



Kritischer Pfad

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

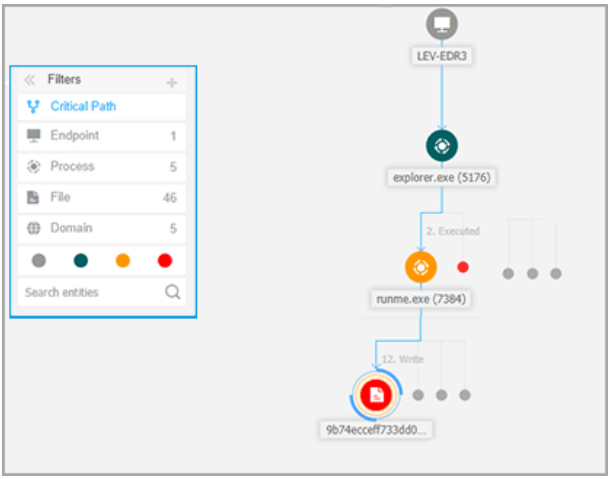
Beachten Sie

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

Filter

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

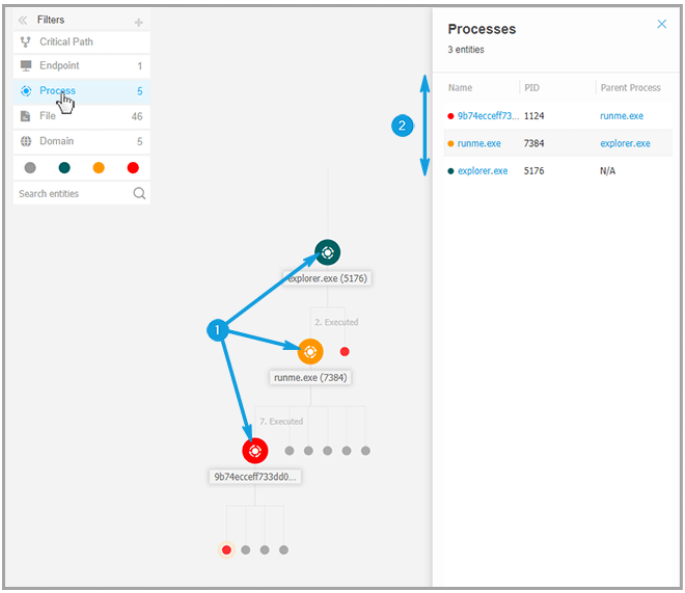
Sie können auf das ✣ **Ziehen**-Symbol klicken und mit festgehaltener Maustaste das schwebende Filterfenster an einer beliebigen Stelle im Vorfallsdiagramm positionieren.



Filtermöglichkeiten im Vorfallsdiagramm

Bei Auswahl eines Filters nach Elementart:

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



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

Die Filteroptionen umfassen:

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

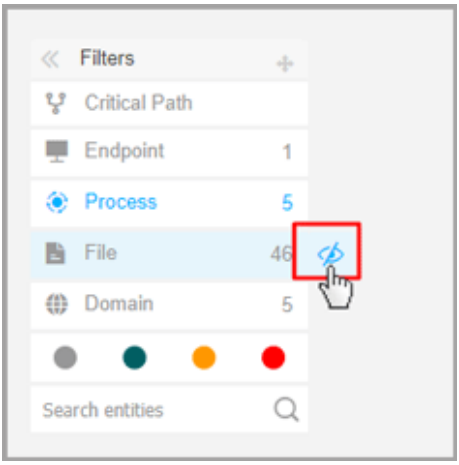
- **Domain**: Hebt alle Knoten vom Typ Domain hervor, die an dem Vorfall beteiligt sind.
- **Registrierung**: Hebt alle Knoten vom Typ Registrierung hervor, die an dem Vorfall beteiligt sind.
- **Elementrelevanz**: Sie können Elemente auch nach ihrer Relevanz für den Vorfall filtern.
  - **Neutraler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

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

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

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

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



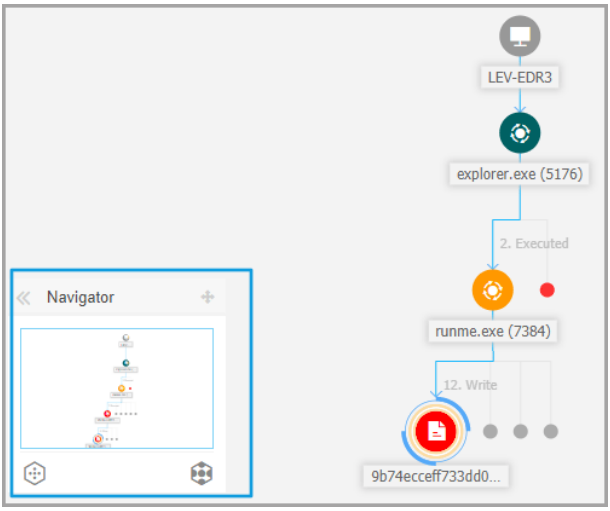
Wird ein Elementtyp ausgeblendet wird die Darstellung des Vorfallsdiagramms aktualisiert. Dabei werden alle entsprechenden Elemente entfernt, auch wenn sie verkleinert dargestellt sind, mit Ausnahme des Auslöserknotens und der Knoten mit untergeordneten Elementen.

Navigation

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

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

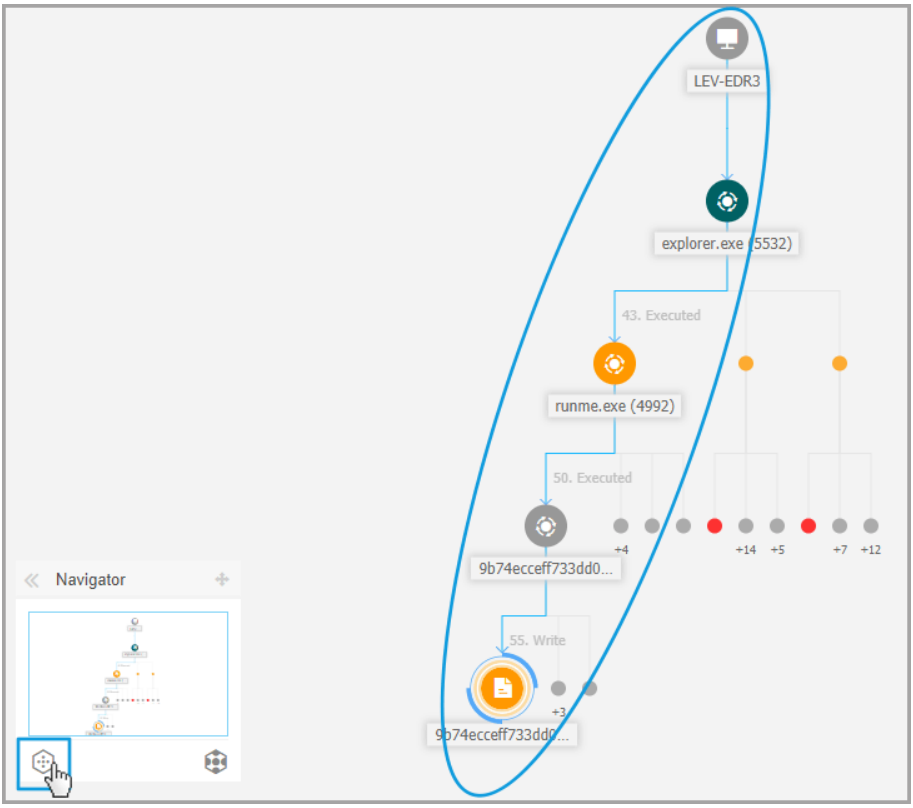
Die **Navigation** wird standardmäßig ausgeblendet. Wird sie erweitert, zeigt das Menü die miniaturisierte Version des gesamten Vorfallsdiagramms und Schaltflächen zur Einstellung der Darstellungsebene an.



Navigation

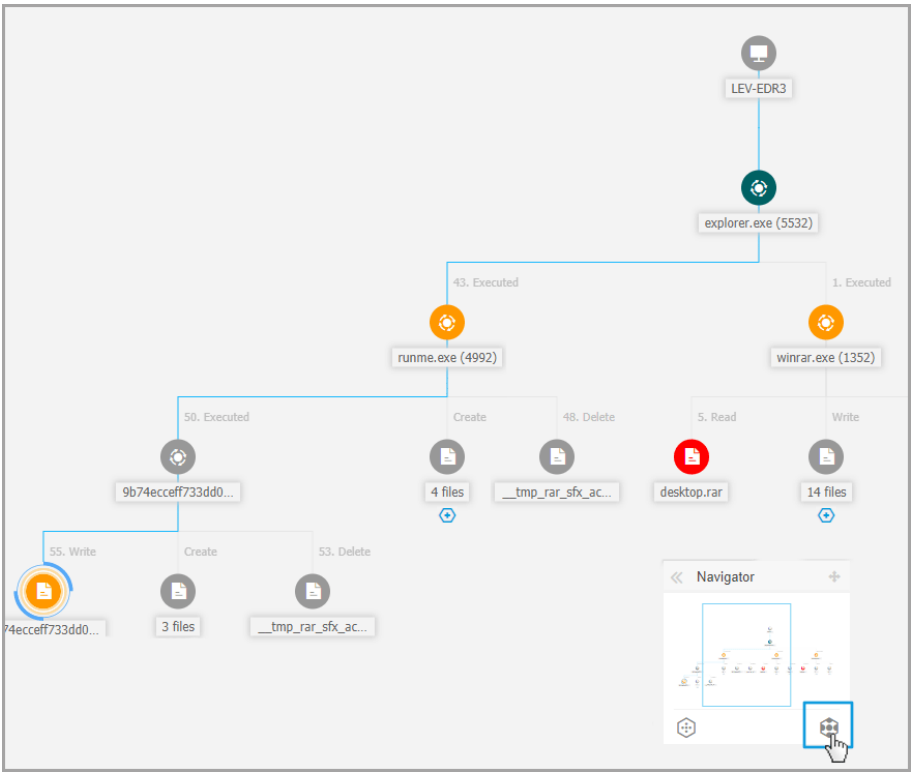
Im **Navigationsmenü** finden Sie zwei Schaltflächen, mit denen Sie festlegen können, wie Sie das Vorfallsdiagramm anzeigen möchten: die Schaltfläche **Weniger Details** und die Schaltfläche **Mehr Details**.

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



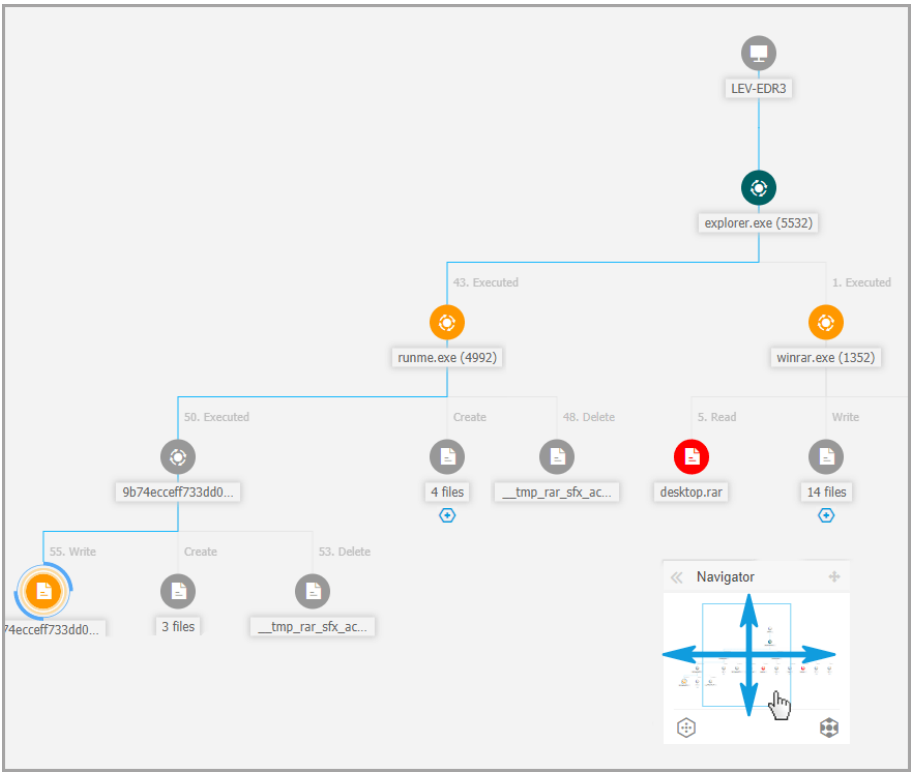
Übersichtsdarstellung

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



Vergrößerte Darstellung

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

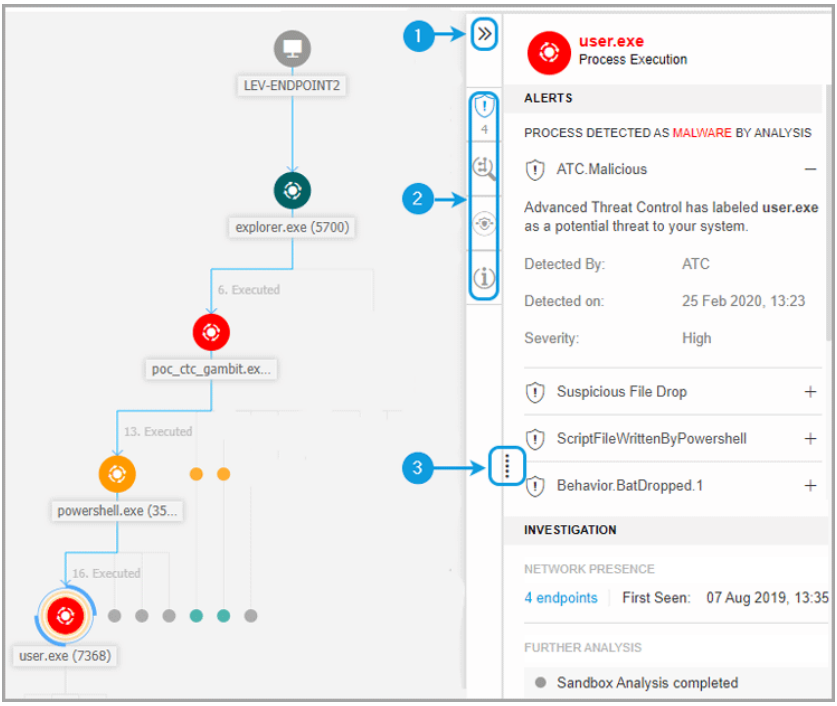


Mini-Karte-Auswahl

Knotendetails

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

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



Bereich Knotendetails

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

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

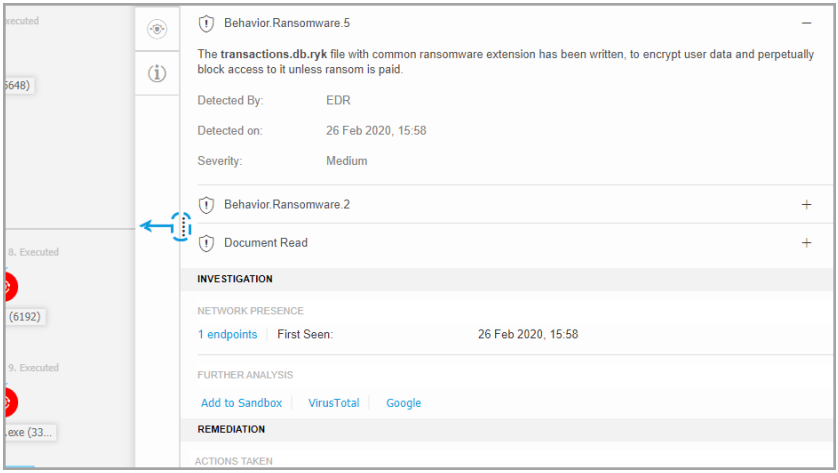
     In diesem Bereich werden die Zeitstempel des ursprünglichen Fundes sowie sämtliche Endpunkte aufgeführt, auf denen dieses Element gefunden wurde.
   - **BEREINIGUNG**

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

- **INFO**

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

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



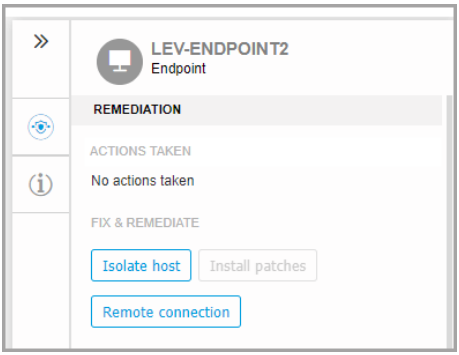
Vergrößerter Bereich Knotendetails

Detailbereich für Endpunkt-Knoten

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

- **BEREINIGUNG**

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

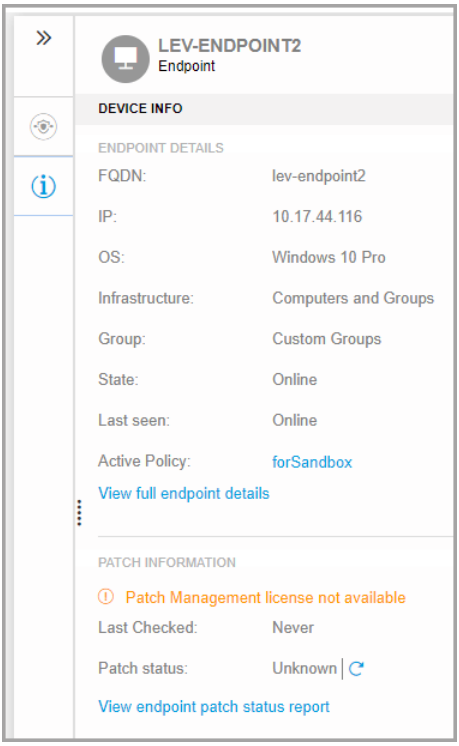


- **Host isolieren** - Mit dieser Aktion isolieren Sie den Endpunkt vom Netzwerk.
- **Installieren von Patches** - Mit dieser Aktion können Sie einen fehlenden Sicherheits-Patch auf dem entsprechenden Endpunkt installieren. Diese Option wird nur angezeigt, wenn das Modul Patch-Verwaltung aktiv ist, das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

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

- **GERÄTE-INFO**

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



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

Auf dieser Tafel können die folgenden Aktionen durchgeführt werden:

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

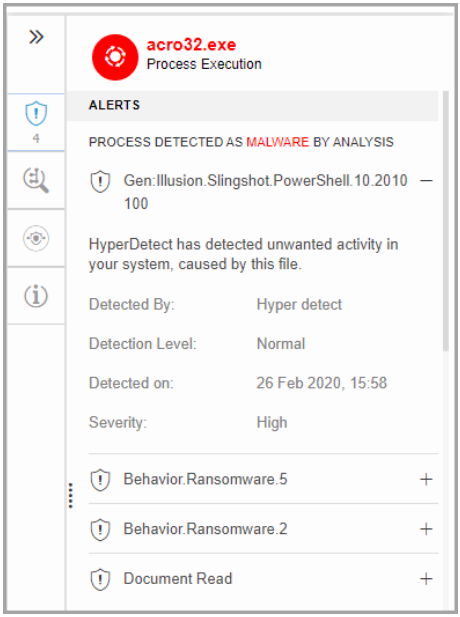
– Den Patch-Statusbericht für den Endpunkt anzeigen. Um den Bericht zu erzeugen, klicken Sie auf **Endpunkt-Patch-Statusbericht anzeigen**.

Detailbereich für Prozess-Knoten

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

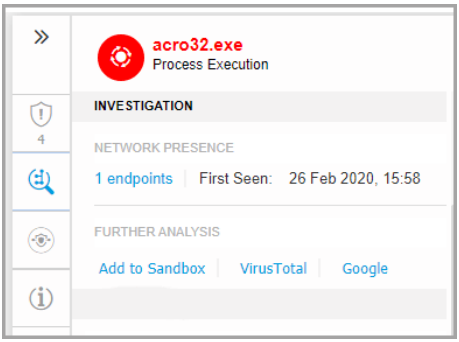
- **WARNMELDUNGEN**

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

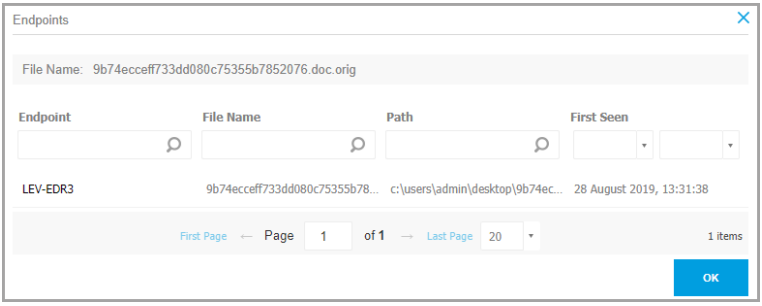


- **UNTERSUCHUNG**

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



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

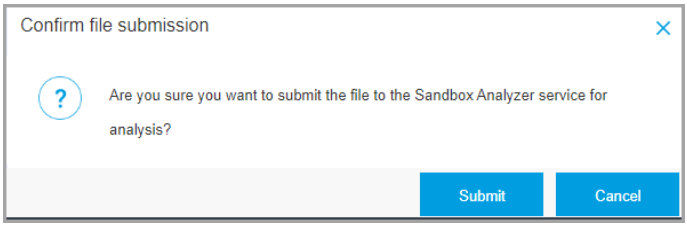


Hier stehen auch Möglichkeiten zur Analyse durch interne Komponenten und externe Lösungen zur Verfügung.

Folgende Aktionen stehen zur Verfügung:

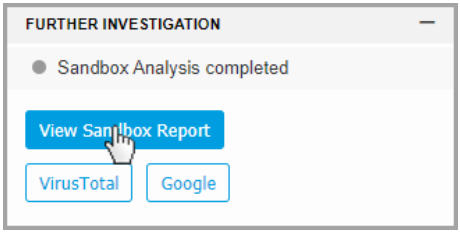
– **Zur Sandbox hinzufügen** - Verwenden Sie diese Aktion, um einen Sandbox Analyzer-Bericht zu erstellen.

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



Nach der Bestätigung werden Sie automatisch zur Übermittlungsseite weitergeleitet.

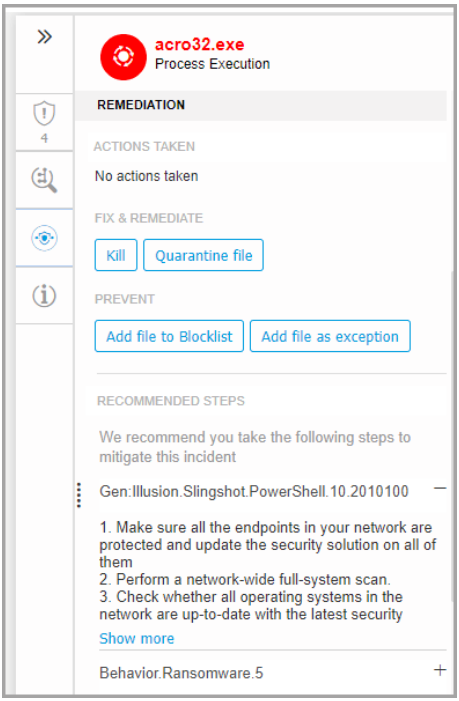
Klicken Sie nach Abschluss der Analyse auf **Sandbox-Bericht anzeigen**, um den vollständigen Bericht zu öffnen.



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

- **BEREINIGUNG**

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



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

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

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

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

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

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

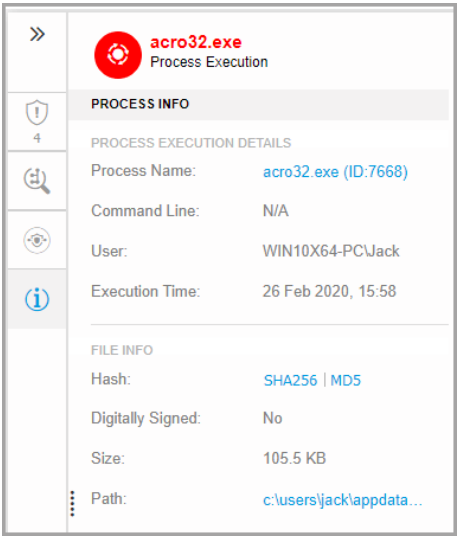
- durch die EDR-Technologie ausgelöste Warnmeldungen
- von einem anderen Prozess erzeugte Knoten
- verdächtige und schädliche Knoten

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

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

- **PROZESS-INFO**

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



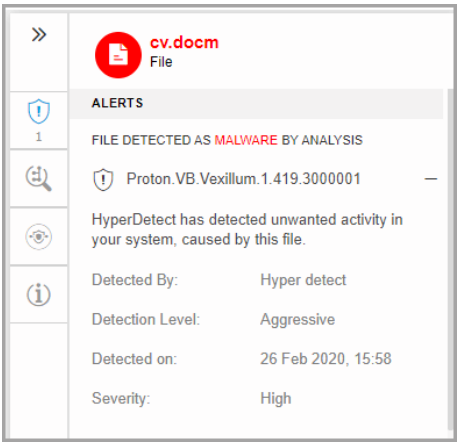
  Wenn Sie den Hash-Wert kopieren möchten, um in an anderer Stelle einfügen zu können, klicken Sie im Feld **Hash** auf die entsprechenden Hash-Algorithmen und anschließend auf **In Zwischenablage kopieren**. Dann können Sie den Hash-Wert einer Datei z. B. in die **Blockierliste** aufnehmen. Näheres hierzu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

Detailbereich für Datei-Knoten

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

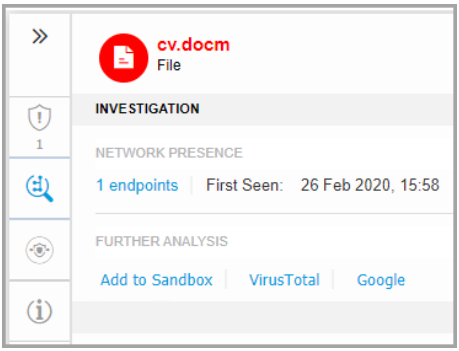
- **WARNMELDUNGEN**

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

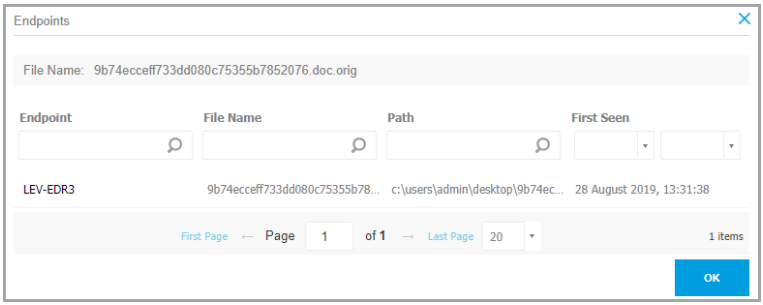


- **UNTERSUCHUNG**

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



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

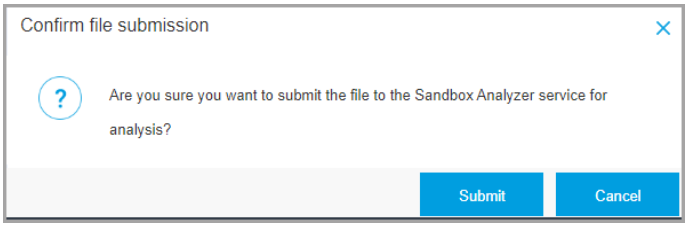


Hier stehen auch Möglichkeiten zur Analyse durch interne Komponenten und externe Lösungen zur Verfügung.

Folgende Aktionen stehen zur Verfügung:

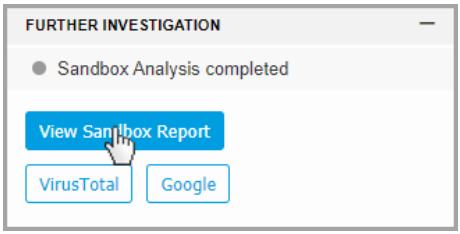
– **Zur Sandbox hinzufügen** - Verwenden Sie diese Aktion, um einen Sandbox Analyzer-Bericht zu erstellen.

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



  Nach der Bestätigung werden Sie automatisch zur Übermittlungsseite weitergeleitet.

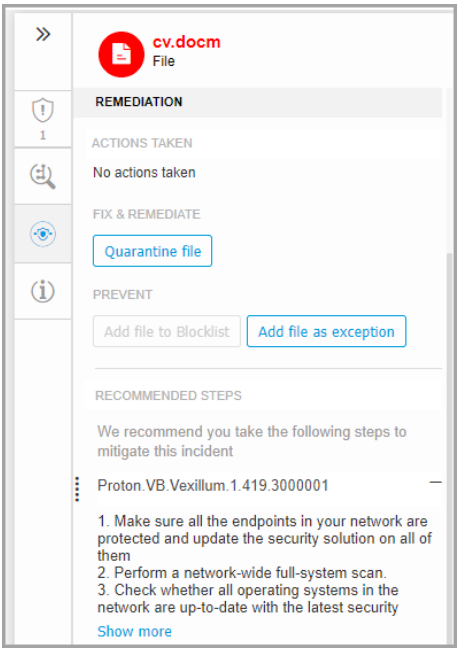
  Klicken Sie nach Abschluss der Analyse auf **Sandbox-Bericht anzeigen**, um den vollständigen Bericht zu öffnen.



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

- **BEREINIGUNG**

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



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

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

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

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

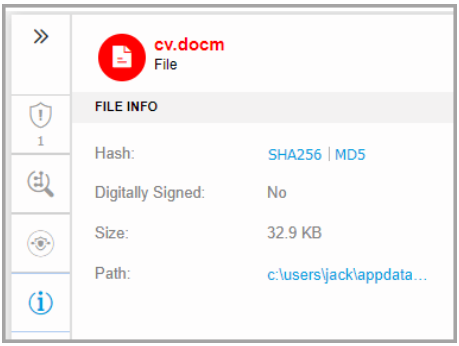
- durch die EDR-Technologie ausgelöste Warnmeldungen
- von einem anderen Prozess erzeugte Knoten
- verdächtige und schädliche Knoten

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

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

- **DATEI-INFO**

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



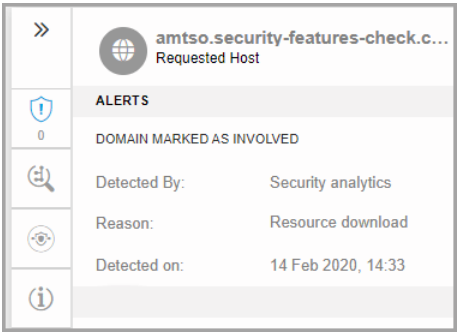
Wenn Sie den Hash-Wert kopieren möchten, um in an anderer Stelle einfügen zu können, klicken Sie im Feld **Hash** auf die entsprechenden Hash-Algorithmen und anschließend auf **In Zwischenablage kopieren**. Dann können Sie den Hash-Wert einer Datei z. B. in die **Blockierliste** aufnehmen. Näheres hierzu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

Detailbereich für Domain-Knoten

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

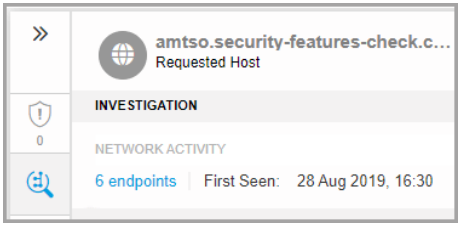
- **WARNMELDUNGEN**

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

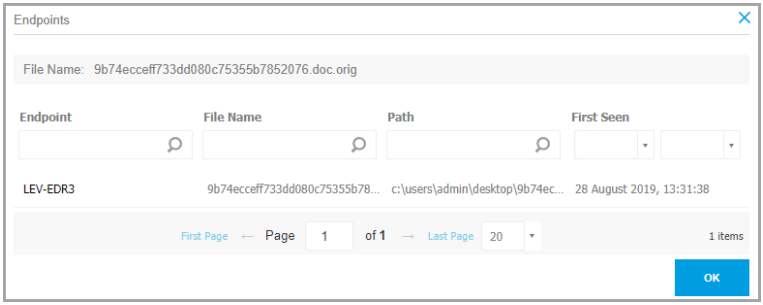


- **UNTERSUCHUNG**

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

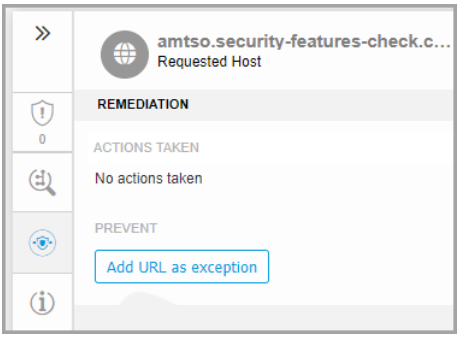


  Diese Liste wird angezeigt, wenn Sie auf die Zahl klicken, die im Feld **Endpunkte** angezeigt wird. Daraufhin wird ein neues Fenster angezeigt.



- **BEREINIGUNG**

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



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

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

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

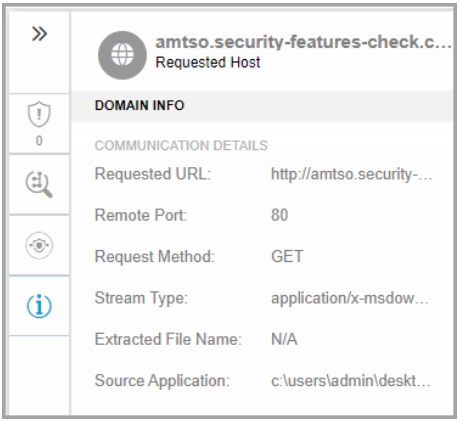
Wichtig
Die Funktion **Als EDR-Ausschluss hinzufügen** ist ausschließlich verfügbar für:

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

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

- **DOMAIN-INFO**

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



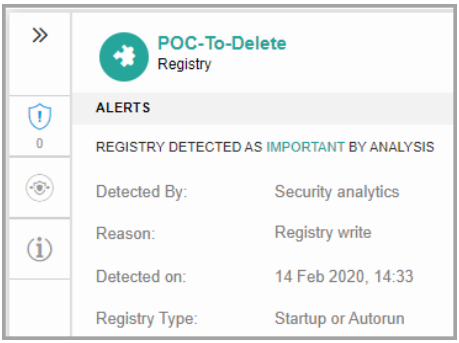
Detailbereich für Registrierungs-Knoten

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

- **WARNMELDUNGEN**

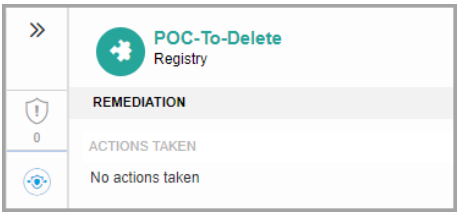
  In diesem Bereich wird der Schweregrad der Registrierungs-Manipulation angezeigt, und zwar gemessen an der Bitdefender-Technologie, mit der die

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



- **BEREINIGUNG**

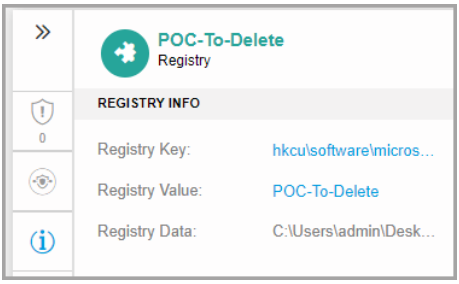
  Hier werden Informationen zu den Aktionen angezeigt, die von GravityZone automatische durchgeführt wurden.



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

- **REGISTRIERUNGS-INFO**

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

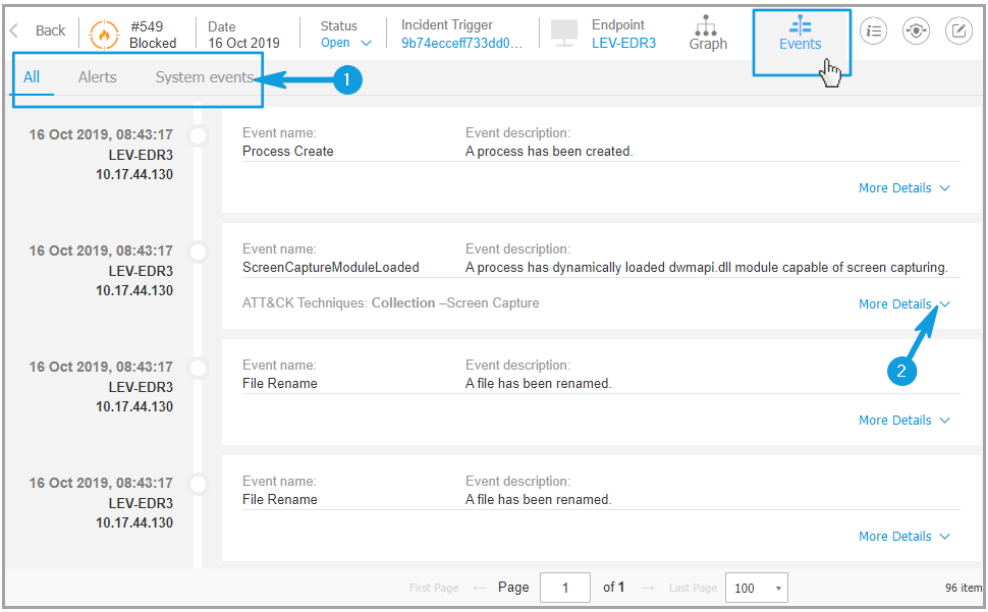


Auf den Schlüssel oder den Wert können Sie klicken, um ihn in die Zwischenablage zu kopieren und an anderer Stelle einfügen zu können.

Ereignisanzeige

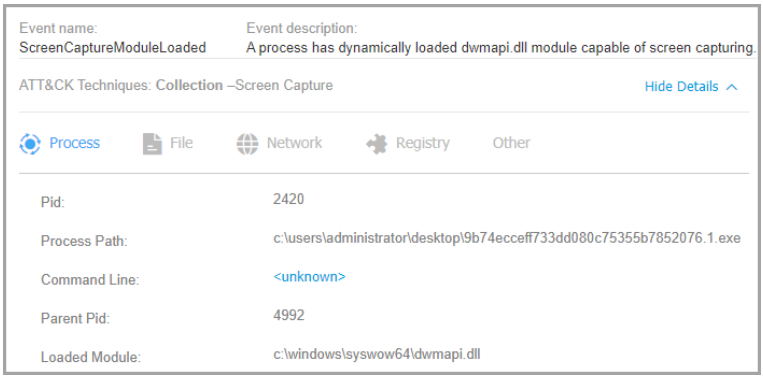
Im Reiter **Ereignisanzeige** können Sie einsehen, welche Abfolge von Ereignissen den aktuell untersuchten Vorfall ausgelöst hat. In diesem Fenster werden die korrelierten Systemereignisse und Warnmeldungen angezeigt, die von GravityZone-Technologien wie EDR,Network Attack Defense, Anomalieerkennung,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

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



Ereignisreiter

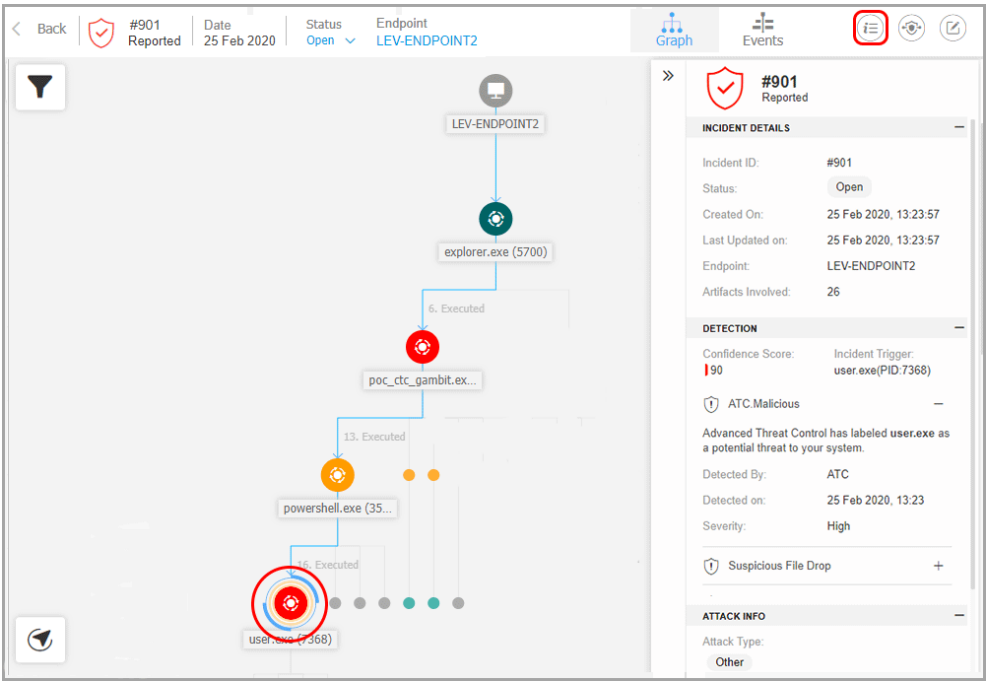
1. Verwenden Sie die Filteroptionen, um alle Ereignisse bzw. entweder nur Systemereignisse oder komplexe Ereignisse (Warnmeldungen) anzuzeigen.
2. Klicken Sie auf die Schaltfläche **Mehr ...**, um die einzelnen Ereignisse zu erweitern und auf zusätzliche Informationen zuzugreifen.



Vorfallsinformationen

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

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

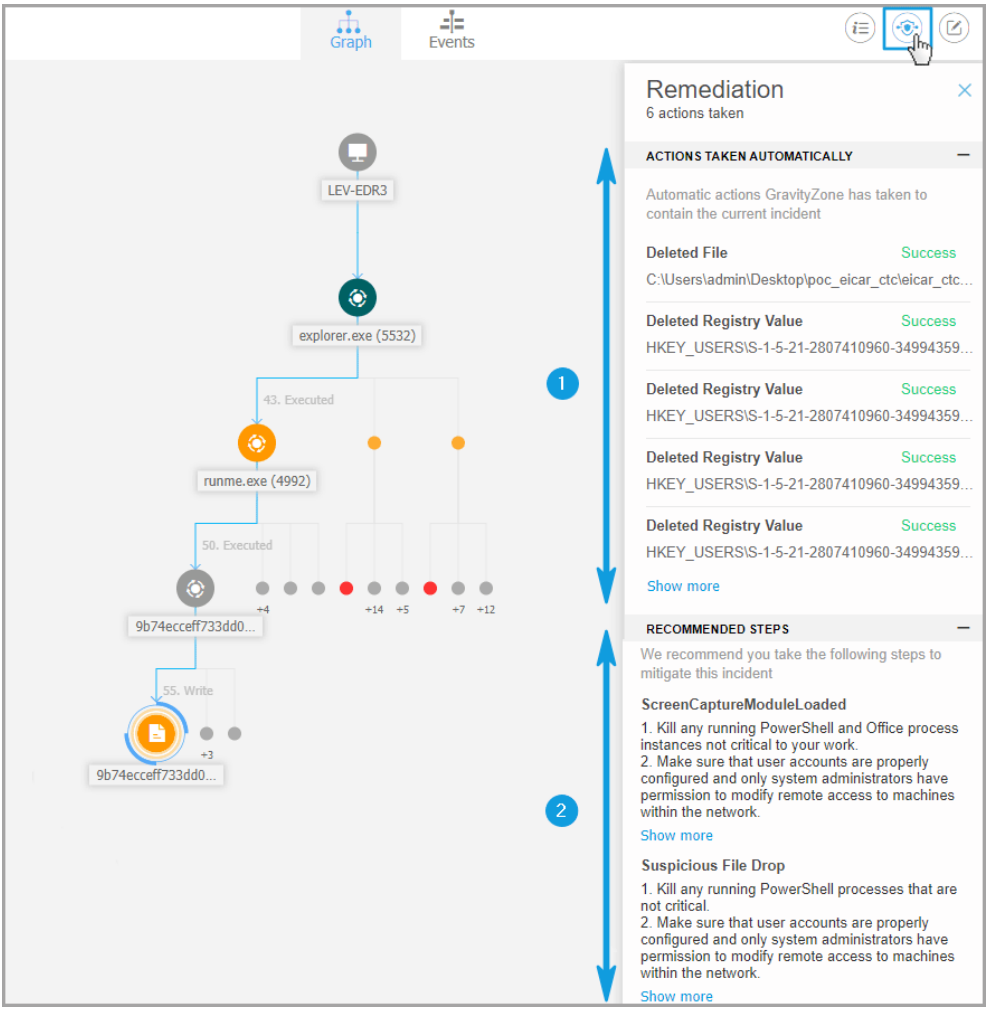


Vorfallsinformationen

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

Bereinigung

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



Bereinigung

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

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

Notizen

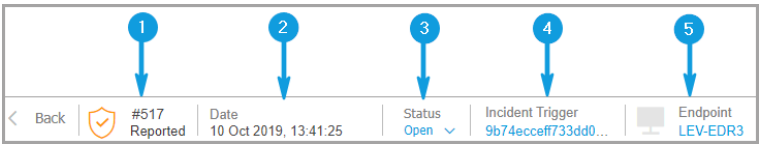
Im Bereich **Notizen** können Sie eigene Notizen hinzufügen, um aktuelle Änderungen nachzuverfolgen und die Delegation von Verantwortlichkeiten für einen Vorfall zu erleichtern.

Zwischenablage für Notizen

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

Vorfallstatusleiste

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



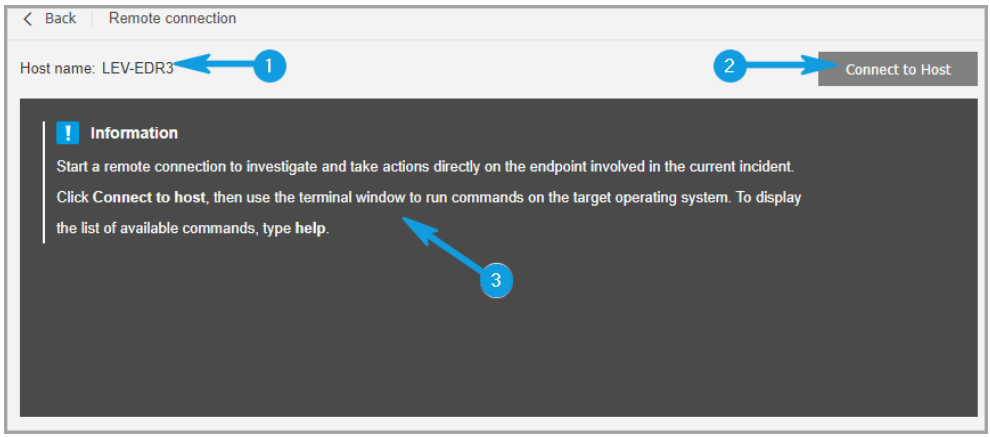
Vorfallstatusleiste

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

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

Remote-Verbindung

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



Der Reiter Remote-Verbindung

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

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

Voraussetzungen für eine Terminalsitzung

- Die auf dem Endpunkt installierte Version des Bitdefender-Agenten unterstützt die Funktion Remote-Verbindung.
- Der Endpunkt muss eingeschaltet und online sein.
- Der Endpunkt muss über ein Windows-Betriebssystem verfügen.

- GravityZone ist zur Kommunikation mit dem Endpunkt in der Lage.
- Ihr GravityZone-Benutzerkonto muss über Verwaltungsberechtigungen für den Zielendpunkt verfügen.

Eine Remote-Verbindung herstellen

So funktioniert die Remote-Verbindung:

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

   Der Verbindungsstatus wird neben dem Endpunktnamen angezeigt.

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

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

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

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

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

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

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

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

   Die Terminalsitzung läuft nach fünf Minuten Inaktivität automatisch ab.

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

Befehle für die Terminalsitzung

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

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

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

    `C:\Users\publ??` listet alle Inhalte des angegebenen Pfades mit beliebigen letzten zwei Buchstaben auf.
  - **Syntax**: `ls [path]`
  - **Aliase**: `dir`

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

- `rm (del, delete)`
  - **Beschreibung**: Löscht Dateien und Ordner aus dem angegebenen Pfad auf dem Zielendpunkt.
  - **Syntax**: `rm [path]`
  - **Aliase**: `del/delete`
  - **Parameter**: `[Path]` - den Pfad zu einer Datei oder einem Ordner auf dem Zielendpunkt.
- `reg query`
  - **Beschreibung**: Gibt alle Informationen (Name, Typ und Wert) für den angegebenen Registrierungsschlüsselpfad zurück.
  - **Syntax**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Aliase**: -
  - **Parameter**:
    - `keypath`- gibt alle Registrierungsschlüsselinformationen aus dem angegebenen Pfad zurück.
    - `/k [keyname]` - filtert die Registrierungsschlüsselergebnisse nach einem bestimmten Schlüsselnamen. Sie können auch Platzhalter (*, ?) verwenden, um nach einem größeren Namensbereich zu filtern.
    - `/v [valuename]` - filtert die Registrierungswerte nach einem bestimmten Wertnamen. Sie können auch Platzhalter (*, ?) im Wertnamen verwenden, um nach einem größeren Namensbereich zu filtern.
- `reg add`
  - **Beschreibung**: Fügt einen neuen Registrierungsschlüssel oder -wert hinzu. Überschreibt einen bereits vorhandenen Registrierungswert. Beim Überschreiben von Registrierungsinformationen müssen Sie alle definierten Parameter angeben.
  - **Syntax**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`

- **Aliase**: -
- **Parameter**:
  - `[keyname]` - der Name des Registrierungsschlüssels.
  - `/v [valuename]` - der Name des Registrierungswerts. Es muss auch mindestens der Parameter /d [data] hinzugefügt werden.
  - `/t [datatype]` - der Datentyp des Registrierungswerts. Sie können einen der folgenden Datentypen hinzufügen:

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

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

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

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

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

    ```
    reg delete [keyname] [/va]
    ```

  - **Aliase**: -
  - **Parameter**:

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

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

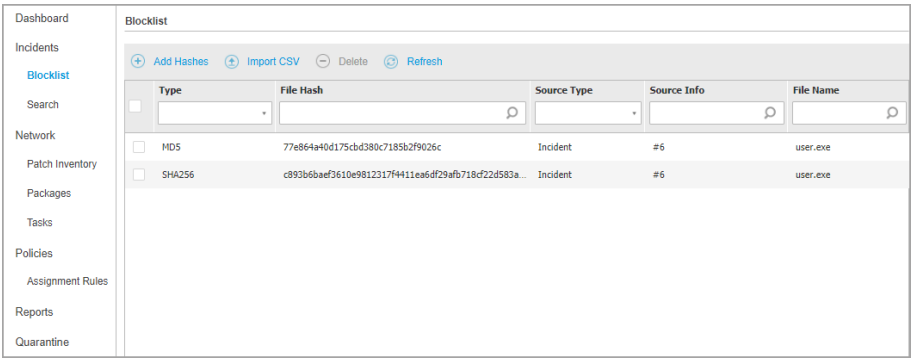
    `/va` - löscht alle Werte des angegebenen Registrierungsschlüssels.

- `cd`
  - **Beschreibung**: Ändert das Arbeitsverzeichnis auf den angegebenen Pfad. Dieser Befehl erfordert als Parameter den Pfad zu einem Laufwerk oder Ordner vom Zielendpunkt aus.
  - **Syntax**: `cd [path]`

  - **Aliase**: -
  - **Parameter**: `[Path]` - den Pfad zu einer Datei oder einem Ordner auf dem Zielendpunkt.
- `hilfe`
  - **Beschreibung**: Ohne Angabe eines Parameters listet help alle verfügbaren Befehle mit einer kurzen Beschreibung auf. Wenn Sie help gefolgt von einem Parameter eingeben, zeigt es die vollständige Syntax dieses Befehls, eine kurze Beschreibung und ein Anwendungsbeispiel an.
  - **Syntax**: `help [command]`
  - **Aliase**: -
  - **Parameter**: Befehlsname (z. B.: `cd, kill, ls, ps`)
- `clear (cls)`
  - **Beschreibung**: Löscht den Inhalt des Terminalfensters und zeigt die Eingabeaufforderung mit dem aktuellen Arbeitsordner an.
  - **Syntax**: `clear`
  - **Aliase**: `cls`
  - **Parameter**: -

6.2. Dateien zur Blockierliste hinzufügen

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



Blockierliste

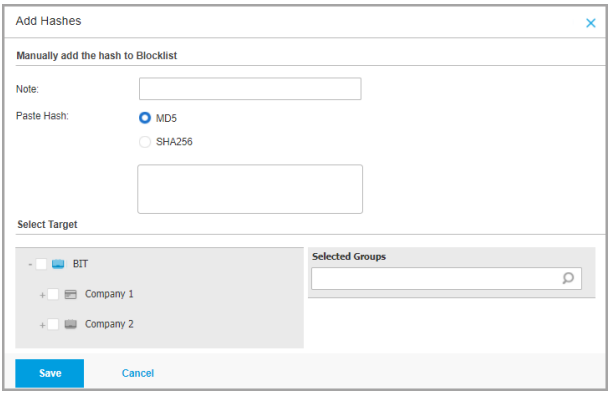
Der Datentabelle können Sie die folgenden Details für jedes Objekt entnehmen:

- Dateitypen:
  - MD5
  - SHA256
- Hashwert der Datei
- Quellentyp:
  - Vorfall (EDR)
  - Importieren
  - Manuell
- Quelleninfo
- Dateiname
- Unternehmen

So fügen Sie Hash-Werte zur bestehenden Blockierliste hinzu:

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

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

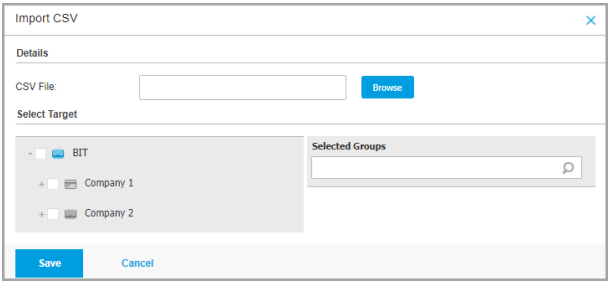


Fenster zum Hinzufügen des Hashwerts

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

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

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



Fenster für den CSV-Import

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

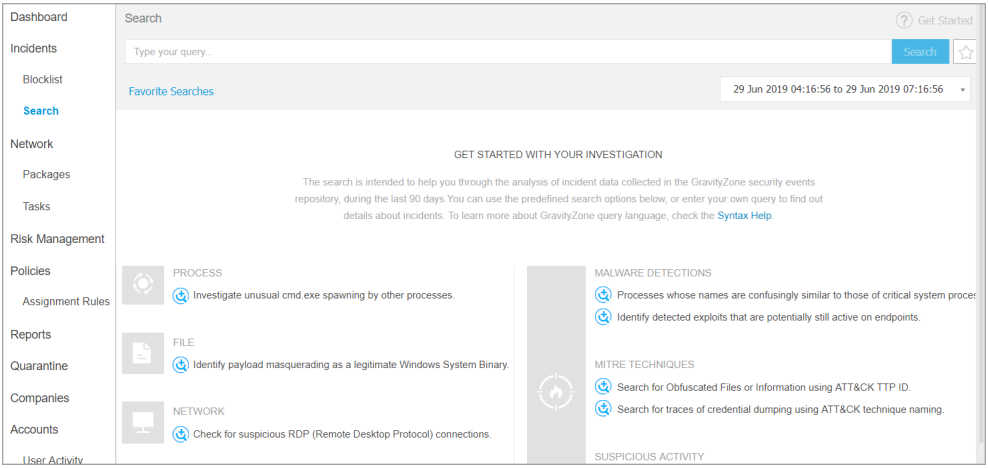
Um eine gültige CSV-Datei für den Import zu erstellen, müssen Sie die ersten drei Spalten mit den folgenden Daten füllen:

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

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

6.3. Sicherheitsereignisse durchsuchen

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



Suchseite

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

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

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

6.3.1. Die Abfragesprache

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

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

Felder

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

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

Operatoren

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

Operator	Beispiel	Beschreibung
`:`	`fieldCategory.option: value1`	Vergleicht den Wert des Abfragefeldes mit den Werten desselben Feldes in der Datenbank.
`" "`	`fieldCategory.option: "value1 value2"`	Zeichenfolgen, die innerhalb von Anführungszeichen stehen, werden als eine Einheit behandelt.

Operator	Beispiel	Beschreibung
`( )`	`fieldCategory1.option: value1 UND (fieldCategory2.option: value2 OR fieldCategory3.option: value3)`	Fasst Abfrageterme zu einer Gruppe zusammen.
`AND`	`fieldCategory1.option: value1 UND fieldCategory2.option: value2`	Zeigt Ergebnisse an, die alle gewählten Abfragebedingungen erfüllen.
`oder`	`fieldCategory1.option: value1 ODER fieldCategory2.option: value2`	Zeigt Ergebnisse an, die beliebig viele der gewählten Abfragebedingungen erfüllen.
`UND NICHT`	`fieldCategory1.option: value1 UND NICHT fieldCategory2.option: value2`	Dieser Operator eignet sich für komplexe Abfragen und liefert neben allen anderen Bedingungen Ergebnisse, die nicht dem angegebenen Begriff entsprechen.
`_exists_`	`_exists_: fieldCategory.option`	Bringt Ergebnisse, die das angegebene Feld beinhalten.
`-`	`fieldCategory.option: -value`	Mit dem Minuszeichen (-) können Werte von den Ergebnissen ausgeschlossen werden.
`?`	`fieldCategory.option: ???_file.path`	Mit einem Fragezeichen (?) kann ein beliebiges Zeichen im Feldwert ersetzt werden.
`*`	`fieldCategory.option: file.*`	Mit einem Asterisk (*) kann ein beliebiger Feldwert ersetzt werden.

Syntax der Abfragen

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

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

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

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

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

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

6.3.2. Abfragen durchführen

So führen Sie eine Abfrage durch:

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

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

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

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

Beachten Sie
Mithilfe verschachtelter Abfragen können Sie komplexe Suchanfragen stellen.

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

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

   Sie haben mehrere Möglichkeiten, den Suchzeitraum festzulegen:

   - Ein bestimmtes Datum.

     Wählen Sie im Reiter **ab** des Kalenders ein Datum.
   - Ein bestimmter Zeitraum.
     a. Legen Sie im Reiter **ab** des Kalenders das Startdatum fest.
     b. Legen Sie im Reiter **Bis** das Enddatum fest.
   - Ein jüngerer Zeitraum aus der verfügbaren Auswahl.
   - Klicken Sie auf **OK**.

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

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

   Wichtig
   Wenn Sie die Abfrage `detections.detection_type` im Feld *Suche* durchführen, müssen Sie in Control Center einen ganzzahligen Wert von 1 bis 15 eingeben (d. h. `detections.detection_type:1`).
   Jeder eingegebene Wert entspricht einem bestimmten Erkennungstyp:
   a. `detections.detection_type:1` - Erkennung mit Advanced Threat Control
   b. `detections.detection_type:2` - Erkennung durch statische Malware-Schutz-Engines
   c. `detections.detection_type:3` - Erkennung durch HyperDetect

d. `detections.detection_type:4` - Benachrichtigung über verdächtige Ereignisse durch Advanced Threat Control
e. `detections.detection_type:5` - Erkennung von Angriffstypen, die von HyperDetect gemeldet wurden
f. `detections.detection_type:6` - Erkennung durch Befehlszeilen-Scanner für Malware-Schutz
g. `detections.detection_type:7` - Erkennung mit Cross Technologies Correlation
h. `detections.detection_name:8` - Erkennung mit Network Attack Defense
i. `detections.detection_type:9` - Erkennung von Angriffstypen, die nicht von HyperDetect gemeldet wurden
j. `detections.detection_type:10` - Erkennung durch eine dynamische Analyse in einer geschlossenen Umgebung mit Sandbox Analyzer
k. `detections.detection_type:11` - Erkennung durch Arbeitsspeicherpuffer-Register-Scan
l. `detections.detection_type:12` - URL-Erkennung
m. `detections.detection_type:13` - Erkennung mit Advanced Anti-Exploit
n. `detections.detection_type:14` - Erkennung durch Analyse des Benutzerverhaltens
o. `detections.detection_type:15` - Erkennung durch Malware-Scan auf der Benutzeroberfläche
p. `detections.detection_type:16` - technologieübergreifender Korrelationsfund auf Grundlage von maschinellem Lernen

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

6.3.3. Suchfavoriten

Viele Abfragen sind lang, und einige sind sehr aufwändig zu erstellen oder schwierig zu merken. Anstatt die Abfragen in einer Datei zu speichern und bei Bedarf nach

GravityZone zu kopieren, können Sie sie für schnellen Zugriff direkt in GravityZone speichern.

So speichern Sie eine Abfrage:

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

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

Hier haben Sie drei Möglichkeiten:

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

So führen Sie eine gespeicherte Abfrage durch:

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

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

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

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

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

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

6.3.4. Vordefinierte Abfragen

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

Vordefinierte Abfragen sind nach Kategorien von Sicherheitsuntersuchungen geordnet.

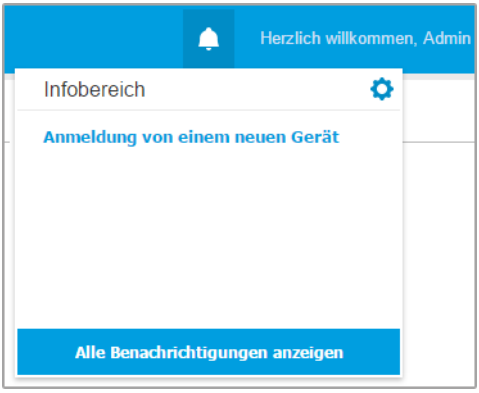
So können Sie eine vordefinierte Abfrage starten:

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

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

7. BENACHRICHTIGUNGEN

Je nach den Ereignissen, die in Ihrem Netzwerk auftreten, wird das Control Center verschiedene Benachrichtigungen anzeigen, die Sie über den Sicherheitsstatus Ihrer Umgebung auf dem Laufenden halten. Die Benachrichtigungen werden im **Infobereich** an der rechten Seite des Control Center angezeigt.



Infobereich

Wenn neue Ereignisse im Netzwerk gefunden werden, zeigt das 11-Symbol oben rechts in der Control Center die Anzahl der gefundenen Ereignisse an. Mit einem Klick auf das Symbol wird der Infobereich mit der Liste der gefundenen Ereignisse angezeigt.

7.1. Benachrichtigungsarten

Hier eine Liste der verfügbaren Benachrichtigungstypen:

Malware-Ausbruch

Diese Benachrichtigung wird an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit derselben Malware infiziert haben.

Im Fenster **Benachrichtigungseinstellungen** können Sie die Malware-Ausbruchschwelle Ihren Bedürfnissen entsprechend konfigurieren. Weitere Informationen finden Sie unter „Benachrichtigungseinstellungen konfigurieren“ (S. 101).

Von HyperDetect gefundene Bedrohungen werden von dieser Benachrichtigung nicht abgedeckt.

Erweiterter Exploit-Schutz
Diese Benachrichtigung wird ausgegeben, wenn der erweiterte Exploit-Schutz Exploit-Versuche in Ihrem Netzwerk erkannt hat.

Anmeldung von einem neuen Gerät
Diese Benachrichtigung informiert Sie darüber, dass über Ihr GravityZone-Konto eine Anmeldung am Control Center von einem Gerät aus erfolgt ist, von dem aus Sie sich bisher noch nicht angemeldet hatten. Die Benachrichtigung wird automatisch so konfiguriert, dass sie sowohl in der Control Center angezeigt als auch per E-Mail verschickt wird und schreibgeschützt ist.

Netzwerkvorfallereignis
Diese Benachrichtigung wird immer dann ausgegeben, wenn das Network Attack Defense-Modul den Versuch eines Angriffs auf Ihr Netzwerk erkennt. Diese Benachrichtigung informiert Sie auch, ob der Angriffsversuch von außerhalb des Netzwerks oder von einem infizierten Endpunkt innerhalb des Netzwerks aus durchgeführt wurde. Weitere Details umfassen Daten zum Endpunkt, zur Angriffstechnik, die IP des Angreifers und die von Network Attack Defense ergriffenen Maßnahmen.

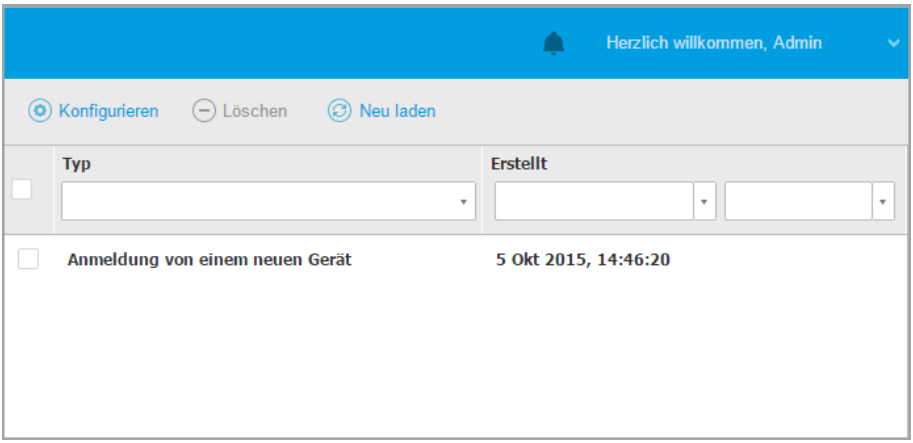
Problem durch fehlenden Patch
Diese Benachrichtigung wird angezeigt, wenn auf Endpunkten in Ihrem Netzwerk ein oder mehrere Patches fehlen.

Sie können überprüfen, für welche Endpunkte dies zutrifft, indem Sie in den Benachrichtigungsdetails auf **Bericht anzeigen** klicken.

Die Benachrichtigung bezieht sich standardmäßig auf sicherheitsrelevante Patches. Sie kann aber auch zur Anzeige von nicht sicherheitsrelevanten Patches konfiguriert werden.

7.2. Benachrichtigungen anzeigen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche **Benachrichtigungen** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.



Die Benachrichtigungsübersicht

Abhängig von der Anzahl der Benachrichtigungen kann sich die Tabelle über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.

Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das Filtermenü über der Tabelle verwenden, um die angezeigten Daten zu filtern.

- Sie können die Benachrichtigungen Filtern, indem Sie den gewünschten Benachrichtigungstyp aus dem Menü **Typ** wählen. Optional können Sie auch den Zeitraum, in dem die Benachrichtigungen erstellt wurden, eingrenzen, um die Zahl der in der Tabelle angezeigten Einträge zu verringern, besonders wenn sehr viele Benachrichtigungen erstellt worden sind.
- Wenn Sie auf den Namen einer Benachrichtigung in der Tabelle klicken, werden weitere Details zu ihr angezeigt. Unter der Tabelle wird der Bereich **Details** angezeigt, in dem das Ereignis angezeigt wird, dass die Benachrichtigung verursacht hat.

7.3. Benachrichtigungen löschen

So löschen Sie Benachrichtigungen:

1. Klicken Sie auf der rechten Seite der Menüleiste auf die Schaltfläche **Benachrichtigung** und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Wählen Sie die Benachrichtigungen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle.

Sie können auch einstellen, dass Benachrichtigungen nach einer bestimmten Anzahl an Tagen gelöscht werden. Weitere Informationen finden Sie im Kapitel „Benachrichtigungseinstellungen konfigurieren“ (S. 101).

7.4. Benachrichtigungseinstellungen konfigurieren

Die Benachrichtigungstypen, die gesendet werden, sowie die E-Mail-Adresse, an die sie gesendet werden, können für jeden Benutzer einzeln festgelegt werden.

So konfigurieren Sie die Benachrichtigungseinstellungen:

1. Klicken Sie auf der rechten Seite der Menüleiste auf die Schaltfläche **Benachrichtigung** und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Konfigurieren** am oberen Rand der Tabelle. Das Fenster **Benachrichtigungsseinstellungen** wird angezeigt.

Benachrichtigungseinstellungen

Beachten Sie
Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

3. Im Bereich **Konfiguration** können Sie die folgenden Einstellungen vornehmen:
   -
   - Zusätzlich können Sie die Benachrichtigungen per E-Mail an bestimmte Empfänger schicken. Geben Sie die E-Mail-Adressen in das vorgesehene Feld ein und drücken Sie nach jeder Adresse `Eingabe`.

4. Im Bereich **Benachrichtigung aktivieren** können Sie festlegen, welche Art von Benachrichtigungen Sie von GravityZone erhalten möchten. Sie können auch für jeden Benachrichtigungstyp einzeln die Anzeige- und Versandoptionen festlegen.

   Wählen Sie einen Benachrichtigungstyp aus der Liste. Weitere Informationen finden Sie im Kapitel „Benachrichtigungsarten“ (S. 98). Solange ein Benachrichtigungstyp ausgewählt ist, können Sie auf der rechten Seite die Optionen (sofern vorhanden) für diesen Typ konfigurieren:

Transparenz

- **Im Control Center anzeigen** legt fest, dass dieser Ereignistyp im Control Center über die Schaltfläche  im **Benachrichtigungen** angezeigt wird.
- **per E-Mail senden**: Dieser Ereignistyp wird auch an bestimmte E-Mail-Adressen gesendet. In diesem Fall müssen Sie die E-Mail-Adressen in das entsprechende Feld eingeben und nach jeder Adresse die `Enter-Taste` drücken.

Konfiguration

- **Benutzerdefinierte Schwelle verwenden** - hiermit kann eine Schwelle für die eingetretenen Ereignisse festgelegt werden, für die die ausgewählte Benachrichtigung gesendet wird.

  Zum Beispiel wird die Malware-Ausbruch-Benachrichtigung standardmäßig an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit der gleichen Malware infiziert haben. Sie können die Malware-Ausbruchschwelle verändern, indem Sie die Option **Benutzerdefinierte Schwelle verwenden** aktivieren und dann den gewünschten Wert in das Feld **Malware-Ausbruchschwelle** eingeben.

- Für **Aufgabenstatus** können Sie den Typ des Status wählen, der diesen Typ von Benachrichtigung auslöst:
  - **Jeden Status** - gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe ausgeführt wurde, unabhängig vom Status.
  - **Nur fehlgeschlagene** – gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe fehlgeschlagen ist.

5. Klicken Sie auf **Speichern**.

8. BERICHTE VERWENDEN

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Netzwerkobjekte zentral erstellen und anzeigen. Die Berichte können zu verschiedenen Zwecken eingesetzt werden, wie zum Beispiel:

- Einhaltung der Unternehmenssicherheitsrichtlinien überwachen und sicherstellen.
- Überprüfung und Bewertung des Netzwerksicherheitsstatus.
- Sicherheitsprobleme, Bedrohungen und Sicherheitslücken im Netzwerk erkennen.
- Sicherheitsvorfälle überwachen
- Bereitstellung von übersichtlichen Daten zur Netzwerksicherheit für die Unternehmensführung.

Es stehen verschiedene Berichtstypen zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten. Diese Informationen werden in übersichtlichen interaktiven Diagrammen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Die Berichte können Daten vom gesamten Netzwerk der verwalteten Netzwerkobjekte beinhalten oder sich auf ausgewählte Gruppen konzentrieren. So können Sie mit einem einzigen Bericht folgendes erfahren:

- Statistische Daten zu allen oder Gruppen von verwalteten Netzwerkobjekten.
- Detailinformationen für jedes verwaltete Netzwerkobjekt.
- Die Liste von Computern, die bestimmte Kriterien erfüllen (zum Beispiel solche, deren Malware-Schutz deaktiviert ist).

Einige Berichte ermöglichen es Ihnen auch, die in Ihrem Netzwerk gefundenen Probleme schnell und unkompliziert zu beheben. So können Sie z. B. direkt aus dem Bericht heraus alle gewünschten Netzwerkobjekte aktualisieren, ohne eine Aktualisierungsaufgabe von der Seite **Netzwerk** ausführen zu müssen.

Alle geplanten Berichte stehen im Control Center zur Verfügung, Sie können sie aber auch auf Ihrem Computer speichern oder per E-Mail versenden.

Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

8.1. Berichtstypen

Für jeden Endpunkttyp stehen eine Reihe von Berichtstypen zur Verfügung:

- Berichte zu Computern und virtuellen Maschinen
- Exchange-Berichte

8.1.1. Berichte zu Computern und virtuellen Maschinen

Im Folgenden werden die verschiedenen Berichttypen für physische und virtuelle Maschinen beschrieben:

Phishing-Schutz-Aktivität

Informiert Sie über die Aktivität des Phishing-Schutz-Moduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten Phishing-Websites auf den ausgewählten Endpunkten sowie den Benutzer anzeigen, der zum Zeitpunkt der letzten Erkennung angemeldet war. Sie können auf die Links in der Spalte **Blockierte Websites** klicken, um die URLs der Websites anzuzeigen, wie oft und wann sie zuletzt blockiert wurden.

Blockierte Anwendungen

Informiert Sie über die Aktivitäten der folgenden Module: Malware-Schutz, Firewall, Inhaltssteuerung, Erweiterter Exploit-Schutz und ATC/IDS. Sie können die Anzahl der blockierten Anwendungen auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Klicken Sie auf die einem Ziel zugehörige Zahl, um weitere Informationen zu den blockierten Anwendungen, der Anzahl der Ereignisse und dem Datum und dem Zeitpunkt des zuletzt blockierten Ereignisses anzuzeigen.

Blockierte Webseiten

Informiert Sie über die Aktivität des Moduls Internet-Zugangssteuerung von Bitdefender Endpoint Security Tools. Für jedes Ziel können Sie die Anzahl der blockierten Websites sehen. Wenn Sie auf eine dieser Zahlen klicken, können Sie zusätzliche Informationen anzeigen:

- URL und Kategorie der Website
- Anzahl der versuchten Aufrufe pro Website
- Datum und Zeitpunkt des letzten Versuchs sowie den Benutzer, der zum Zeitpunkt der Erkennung angemeldet war.
- Gründe für die Blockierung. Hierzu gehören: geplanter Zugriff, Erkennung von Malware, Kategorienfilterung und Blacklists.

Datenschutz

Informiert Sie über die Aktivität des Identitätsschutzmoduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten E-Mails und Websites auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Aktivität der Gerätesteuerung

Informiert Sie über Ereignisse beim Zugriff auf die Endpunkte über überwachte Geräte. Sie können für jeden Zielendpunkt die Anzahl der zugelassenen/blockierten Zugriffs- und Schreibgeschützt-Ereignisse anzeigen. Wenn Ereignisse eingetreten sind, können Sie zusätzliche Informationen dazu anzeigen, indem Sie auf die entsprechenden Zahlen klicken. Angezeigt werden Details zu:

- Auf der Maschine angemeldeter Benutzer
- Gerätetyp und -ID
- Gerätehersteller und Produkt-ID
- Datum und Uhrzeit des Ereignisses.

Status der Endpunktverschlüsselung

Liefert Daten zum Verschlüsselungsstatus der Endpunkte. In einem Kuchendiagramm wird die Anzahl der mit den Verschlüsselungsrichtlinieneinstellungen konformen bzw. nicht-konformen Maschinen dargestellt.

In einer Tabelle unter dem Kuchendiagramm werden unter anderem folgende Details angezeigt:

- Endpunkt-Name.
- Full Qualified Domain Name (FQDN).
- IP-Adresse der Maschine.
- Betriebssystem.
- Konformität mit der Geräterichtlinie:
  - **Konform** – wenn sämtliche Laufwerke verschlüsselt oder unverschlüsselt sind, je nach Richtlinie.
  - **Nicht-konform** – wenn der Status des Laufwerks nicht mit der zugewiesenen Richtlinie übereinstimmt (z. B. nur eins von zwei

Laufwerken verschlüsselt ist oder ein Verschlüsselungsvorgang gerade noch auf dem Laufwerk läuft).

- Geräterichtlinie (**Verschlüsseln** oder **Entschlüsseln**).
- Klicken Sie auf die Zahlen in der Spalte Laufwerkzusammenfassung, um Informationen zu den Laufwerken jedes Endpunkts zu erhalten: ID, Name, Verschlüsselungsstatus (**Verschlüsselt** oder **Unverschlüsselt**), Probleme, Typ (**Boot** oder **Nicht boot-fähig**), Größe, Wiederherstellungsschlüssel-ID.
- Unternehmensname.

Status der Endpunktmodule

Ermöglicht einen Überblick über die Abdeckung durch Sicherheitsmodule auf den ausgewählten Zielen. In den Berichtsdetails können Sie für jeden Zielendpunkt anzeigen, welche Module aktiv, deaktiviert oder nicht installiert sind und welche Scan-Engine verwendet wird. Mit einem Klick auf den Namen des Endpunkts öffnen Sie das Fenster **Informationen**, in dem Sie Details zum Endpunkt und den installierten Schutzebenen finden.

Mit einem Klick auf **Client neu konfigurieren** können Sie eine Aufgabe starten, um die Anfangseinstellungen eines oder mehrerer ausgewählter Endpunkte zu ändern. Einzelheiten finden Sie unter Client neu konfigurieren.

Status des Endpunktschutzes

Bietet Ihnen verschiedene Statusinformationen zu ausgewählten Endpunkten in Ihrem Netzwerk.

- Status des Malware-Schutzes
- Update-Status von Bitdefender Endpoint Security Tools
- Status der Netzwerkaktivität (online/offline)
- Verwaltungsstatus

Sie können nach Sicherheitsaspekt und -status filtern, um die Informationen zu erhalten, nach denen Sie suchen.

Firewallaktivität

Informiert Sie über die Aktivität des Firewall-Moduls von Bitdefender Endpoint Security Tools. Sie können die Anzahl der blockierten Verbindungsversuche und Port-Scans auf den ausgewählten Endpunkten sowie den Benutzer einsehen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

HyperDetect-Aktivität

Informiert Sie über die Aktivität des HyperDetect-Moduls von Bitdefender Endpoint Security Tools.

Im Diagramm im oberen Bereich der Berichtsseite werden die Dynamiken des Angriffsversuchs während des festgelegten Zeitraums sowie die Verteilung der Angriffsarten angezeigt. Wenn Sie mit dem Mauszeiger über die Einträge in der Legende fahren, wird die entsprechende Angriffsart im Diagramm hervorgehoben. Wenn Sie auf einen Eintrag klicken, wird die entsprechende Zeile im Diagramm angezeigt bzw. ausgeblendet. Wenn Sie auf eine beliebige Stelle einer Zeile klicken, werden die Daten in der Tabelle gemäß dem ausgewählten Typ gefiltert. Wenn Sie zum Beispiel an irgendeiner Stelle auf die orangefarbene Zeile klicken, werden in der Tabelle nur Exploits angezeigt.

Über die Details im unteren Bereich des Berichts können Sie die Schwachstellen in Ihrem Netzwerk identifizieren und nachsehen, ob sie behoben wurden. Sie beziehen sich auf:

- Der Pfad zu der Malware-Datei bzw. die gefundene URL im Falle von infizierten Dateien. Bei dateilosen Angriffen wird der Name der für den Angriff verwendeten ausführbaren Datei zusammen mit einem Link zu einem Detailfenster mit Informationen zum Grund der Erkennung und der schädlichen Befehlszeilen-Zeichenfolge angezeigt.
- Der Endpunkt, auf dem der Fund gemacht wurde
- das Sicherheitsmodul, das die Bedrohung gefunden hat. Da HyperDetect eine zusätzliche Schicht der Module Malware-Schutz und Inhaltssteuerung ist, enthält der Bericht Informationen im Zusammenhang mit einem dieser beiden Module. Welche, hängt von der Art des Fundes ab.
- Der Art des beabsichtigten Angriffs (gezielter Angriff, Grayware, Exploit, Ransomware, verdächtige Dateien und Netzwerkdatenverkehr)
- Der Bedrohungsstatus
- Der Sicherheitsstufe, auf der die Bedrohung entdeckt wurde (tolerant, normal, aggressiv)
- die Anzahl der Male, die die Bedrohung gefunden wurde
- der jüngste Fund
- Erkennung als dateiloser Angriff (ja oder nein), um die Funde von dateilosen Angriffen schnell und einfach filtern zu können

Beachten Sie
Eine Datei kann in verschiedenen Angriffen vorkommen. Daher meldet GravityZone sie für jede Angriffsart, in der sie vorkam.

In diesem Bericht können Sie Fehlalarme einfach ausschließen, indem Sie in den zugewiesenen Sicherheitsrichtlinien Ausnahmen definieren. Hierzu müssen Sie:

1. Wählen Sie so viele Einträge in der Tabelle aus, wie Sie brauchen.

   Beachten Sie
   Die Erkennung von dateilosen Angriffen kann nicht zur Liste der Ausnahmen hinzugefügt werden, da es sich bei der gefundenen ausführbaren Datei selbst nicht um Malware handelt. Sie kann vielmehr zu einer Bedrohung werden, wenn eine schädliche codierte Befehlszeile zum Einsatz kommt.

2. Klicken Sie auf die Schaltfläche **Ausnahme hinzufügen** am oberen Ende der Tabelle.
3. Wählen Sie im Konfigurationsfenster die Richtlinien, zu denen die Ausnahme hinzugefügt werden soll und klicken Sie anschließend auf **Hinzufügen**.

   Informationen über die hinzugefügten Ausnahmen werden standardmäßig an die Bitdefender-Labs übermittelt, um die Erkennungsmöglichkeiten der Bitdefender-Produkte zu verbessern. Diese Option kann über das Kästchen **Übermitteln Sie dieses Feedback an Bitdefender für eine bessere Analyse** ein- und ausgeschaltet werden.

Wenn die Bedrohung vom Malware-Schutz-Modul gefunden wurde, gilt die Ausnahme für Zugriff- und Bedarf-Scans.

Beachten Sie
Sie finden die Ausnahmen in den folgenden Bereichen der ausgewählten Richtlinien: **Malware-Schutz > Einstellungen** für Dateien und **Inhaltssteuerung > Datenverkehr** für URLs.

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Endpunkte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde. Sie können auch den Benutzer anzeigen, der zum Zeitpunkt der letzten Erkennung angemeldet war.

Endpunkte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Endpunkte ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Endpunkte mit behobener Malware (alle als infiziert erkannte Dateien wurden erfolgreich desinfiziert oder in die Quarantäne verschoben)
- Endpunkte mit nicht behobener Malware (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Für jeden Endpunkt können Sie die Liste der Bedrohungen und der betroffenen Dateipfade anzeigen, indem Sie in den Spalten der Desinfektionsergebnisse auf die entsprechenden Links klicken.

In diesem Bericht können Sie schnell einen vollständigen System-Scan auf den Zielen ausführen, auf denen noch keine Behebung durchgeführt wurde, indem Sie in der Symbolleiste über der Datentabelle auf die Schaltfläche **Infizierte Ziele scannen** klicken.

Monatslizenznutzung

Wenn Sie auf die Zahlen in den Spalten klicken, werden Details zu den verschiedenen Modulen und Add-ons angezeigt. Sie können den Inhalt des Berichts ganz einfach anpassen, indem Sie auf die Schaltfläche **Spalten ein-/ausblenden** klicken.

Monatslizenznutzung für Email Security

In diesem Bericht sind Informationen zur Nutzung der Monatslizenzen für den Dienst cloud_email_sec] zusammengefasst. In jedem Bericht sind sämtliche Nutzungsinformationen bis zum Ende des vergangenen Tages enthalten. Sagen wir, Sie erstellen an einem Montag um 12 Uhr mittags einen Bericht und stellen den Zeitraum auf **Dieser Monat** ein. Der erstellte Bericht enthält dann sämtliche Lizenznutzungsinformationen bis einschl. Sonntag 23:59 Uhr.

Netzwerkvorfälle

Informiert Sie über die Aktivitäten des Network Attack Defense-Moduls. Ein Diagramm zeigt die Anzahl der Angriffsversuche, die über einen bestimmten Zeitraum erkannt wurden. Die Berichtsdetails umfassen:

- Endpunktname, IP und FQDN
- Nutzername
- Name des Fundes
- Angriffstechnik
- Anzahl der Versuche
- IP des Angreifers
- Betroffene IP und Port

- Wann der Angriff zuletzt blockiert wurde

Wenn Sie bei einem Fund auf die Schaltfläche **Ausnahmen hinzufügen** klicken, wird automatisch ein Eintrag unter **Global Ausschlüsse** im Bereich **Netzwerkschutz** angelegt.

Patch-Status im Netzwerk

Prüfen Sie den Update-Status der in Ihrem Netzwerk installierten Software. Der Bericht liefert die folgenden Informationen:

- Zielmaschine (Endpunktname, IP und Betriebssystem).
- Sicherheitsrelevante Patches (installierte Patches, fehlgeschlagene Patches und nicht sicherheitsrelevante Patches).
- Status und Zeitpunkt der letzten Änderung für ausgecheckte Endpunkte.

Netzwerkschutzstatus

Zeigt detaillierte Information zum allgemeinen Sicherheitsstatus der Zielendpunkte. Hier finden Sie zum Beispiel folgende Informationen:

- Name, IP und FQDN
- Status:
  - **Hat Probleme** - Auf dem Endpunkt gibt es Schutzlücken (Sicherheitsagent nicht auf dem neuesten Stand, Sicherheitsbedrohungen entdeckt usw.)
  - **Keine Probleme** - Der Endpunkt ist geschützt und es gibt keinen Grund zur Besorgnis.
  - **Unbekannt** - Der Endpunkt war zum Zeitpunkt der Berichterstellung offline.
  - **Nicht verwaltet** - Der Sicherheitsagent wurde bisher noch nicht auf dem Endpunkt installiert.
- Verfügbare Sicherheitsebenen
- Verwaltete und nicht verwaltete Endpunkte (Sicherheitsagent ist installiert oder nicht)
- Lizenztyp und -status (weitere Spalten mit Lizenzinformationen sind standardmäßig ausgeblendet)
- Infektionsstatus (der Endpunkt ist "sauber" oder nicht)
- Update-Status des Produkts und der Sicherheitsinhalte

- Software-Sicherheitspatch-Status (fehlende sicherheitsrelevante und nicht sicherheitsrelevante Patches)

Bei nicht verwalteten Endpunkten sehen Sie den Status **Nicht verwaltet** unter weiteren Spalten.

Prüfvorgang

Liefert Informationen zu den Bedarf-Scans, die auf den ausgewählten Zielen durchgeführt wurden. Eine Statistik der erfolgreichen und fehlgeschlagenen Scans wird in einem Kuchendiagramm angezeigt. In der Tabelle unter dem Diagramm werden Details zum Scan-Typ, zum letzten Auftreten und zum letzten erfolgreichen Scan für jeden Endpunkt angezeigt.

Richtlinienkonformität

Liefert Informationen zu den Sicherheitsrichtlinien, die auf den ausgewählten Zielen angewendet werden. Der Status der Richtlinie wird in einem Kuchendiagramm angezeigt. Der Tabelle unter der Grafik können Sie die jedem Endpunkt zugewiesene Richtlinie und den Richtlinientyp sowie das Datum und den zuweisenden Benutzer entnehmen.

Sandbox Analyzer – Fehlgeschlagene Übermittlungen

Zeigt alle fehlgeschlagenen Übermittlungen von Objekten an, die während eines bestimmten Zeitraums von den Endpunkten an den Sandbox Analyzer gesendet wurden. Eine Übermittlung gilt nach mehreren Versuchen als fehlgeschlagen.

In der Grafik wird die Variation der fehlgeschlagenen Übertragungen während des festgelegten Zeitraums dargestellt. In der Detailtabelle des Berichts werden die Dateien aufgeführt, die nicht an den Sandbox Analyzer gesendet werden konnten, außerdem die Maschine, von der aus das Objekt gesendet wurde, Datum und Uhrzeit jedes erneuten Versuchs, der zurückgegebene Fehlercode, die Beschreibung jedes fehlgeschlagenen Versuchs und der Unternehmensname.

Sandbox Analyzer-Ergebnisse (veraltet)

Liefert detaillierte Informationen zu den Dateien auf den entsprechenden Endpunkten, die in der Sandbox während eines bestimmten Zeitraums analysiert wurden. In einem Liniendiagramm wird die Anzahl der unbedenklichen und die der gefährlichen analysierten Dateien angezeigt, und in einer Tabelle sind Details zu jedem Fall aufgeführt.

Sie können für alle analysierten Dateien oder nur für die als schädlich eingestuften Dateien einen Sandbox Analyzer-Ergebnisbericht erstellen.

Sie können Folgendes sehen:

- Ergebnis der Analyse, also die Information, ob die Datei unbedenklich, gefährlich oder unbekannt (**Bedrohung gefunden** oder **Keine Bedrohung gefunden** oder **Nicht unterstützt**) ist. Diese Spalte wird nur angezeigt, wenn Sie im Bericht alle analysierten Objekte anzeigen lassen.

  Eine vollständige Liste der vom Sandbox Analyzer unterstützten Dateitypen und -erweiterungen finden Sie hier: „Unterstützte Dateitypen und Dateiendungen für die manuelle Übermittlung“ (S. 132).
- Bedrohungstyp, z. B. Adware, Rootkit, Downloader, Exploit, Host-Modifier, Schad-Tools, Passwort-Stehler, Ransomware, Spam oder Trojaner.
- Datum und Uhrzeit des Fundes, wonach Sie je nach Berichtszeitraum filtern können.
- Hostname oder IP-Adresse des Endpunkts, auf dem die Datei gefunden wurde.
- Name der Dateien, wenn sie einzeln übermittelt wurden, oder Anzahl der analysierten Dateien im Fall einer gebündelten Übermittlung. Wenn Sie auf den Dateinamen oder auf den Link des Bündels klicken, werden Details und ausgeführte Aktionen angezeigt.
- Status der Bereinigungsaktion für die übertragenen Dateien (**Teilweise**, **Fehlgeschlagen**, **Nur berichtet**, **Erfolgreich**).
- Unternehmensname.
- Weitere Informationen zu den Eigenschaften der analysierten Datei erhalten Sie, wenn Sie in der Spalte **Analyseergebnis** auf die Schaltfläche **Mehr** klicken. Hier werden Sicherheitsaspekte und das Verhalten der untersuchten Datei im Detail angezeigt.

Der Sandbox Analyzer zeichnet die folgenden Ereignisse auf:

- Schreiben, Löschen, Verschieben, Kopieren, Ersetzen von Dateien im System und auf tragbaren Datenträgern.
- Ausführen von neu erstellten Dateien.
- Änderungen am Dateisystem.
- Änderungen an den laufenden Anwendungen innerhalb einer virtuellen Maschine.
- Änderungen an der Windows-Taskleiste und am Startmenü.
- Erstellen, Beenden, Injizieren von Prozessen.
- Schreiben oder Löschen von Registrierungsschlüsseln.
- Erstellen von Mutex-Objekten.
- Erstellen, Starten, Anhalten, Modifizieren, Abfragen, Löschen von Diensten.
- Ändern der Browser-Sicherheitseinstellungen.

- Änderung der Windows-Explorer-Anzeigeeinstellungen.
- Hinzufügen von Dateien zur Firewall-Ausnahmeliste.
- Änderung von Netzwerkeinstellungen.
- Aktivieren einer Ausführung beim Systemstart.
- Herstellen einer Verbindung zu einem entfernten Host.
- Zugriff auf bestimmte Domains.
- Transfer von Daten von und zu bestimmten Domains.
- Zugriff auf URLs, IP-Adressen und Ports über verschiedene Kommunikationsprotokolle.
- Überprüfen der Indikatoren virtueller Umgebungen.
- Überprüfen der Indikatoren von Überwachungstools.
- Erstellen von Bildschirm- oder Systemabbildern.
- SSDT, IDT, IRP-Hooks.
- Speicherabbilder für verdächtige Prozesse.
- Windows-API-Funktionsaufrufe.
- Wechsel in die Inaktivität für einen bestimmten Zeitraum zur Verzögerung der Ausführung.
- Erstellen von Dateien, die in bestimmten zeitlichen Intervallen auszuführende Aktionen beinhalten.

Klicken Sie im Fenster **Analyseergebnis** auf die Schaltfläche **Download**, um auf Ihrem Computer den Inhalt der Verhaltenszusammenfassung in einem der folgenden Formate zu speichern: XML, HTML, JSON, PDF.

Sicherheitsüberprüfung

Liefert Informationen zu Sicherheitsereignissen auf einem ausgewählten Ziel. Die Informationen beziehen sich auf die folgenden Ereignisse:

- Malware-Erkennung
- Blockierte Anwendung
- Blockierter Scan-Port
- Blockierter Datenverkehr
- Blockierte Website
- Gerät blockieren
- Blockierte E-Mail
- Blockierter Prozess
- Erweiterter Exploit-Schutz-Ereignisse
- Network Attack Defense-Ereignisanzeige

Security Server-Status

Hiermit können Sie den Status eines Security Server bewerten. Verschiedene Statusindikatoren helfen Ihnen dabei, etwaige Probleme eines Security Server zu identifizieren:

- **Status**: Zeigt den allgemeinen Status des Security Servers an.
- **Maschinen-Status**: zeigt an, welche Security Server-Appliances angehalten wurden.
- **AV-Status**: zeigt an, ob das Malware-Schutz-Modul aktiviert oder deaktiviert ist.
- **Update-Status**: zeigt an, ob die Security Server-Appliances auf dem neuesten Stand sind oder ob Updates deaktiviert wurden.
- **Auslastungsstatus**: Zeigt den Scan-Auslastungsgrad eines Security Server wie hier beschrieben an:
  - **Unterbelastet**, wenn weniger als 5 % der Scan-Kapazität verwendet werden.
  - **Normal**, wenn die Scan-Last ausgeglichen ist.
  - **Überlastet**, wenn die Scan-Last 90 % ihrer Kapazität übersteigt. Überprüfen Sie in einem solchen Fall die Sicherheitsrichtlinien. Falls alle Security Server überlastet sind, die innerhalb einer Richtlinie zugeordnet wurden, müssen Sie der Liste einen weiteren Security Server hinzufügen. Überprüfen Sie andernfalls die Netzwerkverbindung zwischen den Clients und den Security Servern ohne Lastprobleme.

Darüber hinaus können Sie die Anzahl der mit dem Security Server verbundenen Agenten einsehen. Mit einem Klick auf die Zahl der verbundenen Clients wird die Liste der Endpunkte angezeigt. Diese Endpunkt könnten für Angriffe anfällig sein, wenn Probleme mit dem Security Server auftreten.

Top-10 der gefundenen Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den ausgewählten Endpunkten gefunden wurden.

> **Beachten Sie**
> In der Detailtabelle werden alle Endpunkte angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Top-10 der infizierten Endpunkte

Zeigt von den ausgewählten Endpunkten die 10 mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.

> **Beachten Sie**
> In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Endpunkten gefunden wurde.

Update-Status

Zeigt Ihnen den Update-Status des auf ausgewählten Zielen installierten Sicherheitsagenten oder Security Server an. Der Update-Status bezieht sich auf das Produkt und die Versionen der Sicherheitsinhalte.

Über die verfügbaren Filter können Sie schnell feststellen, welche Clients in den letzten 24 Stunden aktualisiert und welche nicht aktualisiert wurden.

In diesem Bericht können Sie schnell die Agenten auf die neueste Version aktualisieren. Klicken Sie dazu in der Symbolleiste über der Datentabelle auf die Schaltfläche **Update**.

Upgrade-Status

Zeigt an, welche Sicherheitsagenten auf den ausgewählten Zielen installiert sind und ob es eine neuere Version dazu gibt.

Auf Endpunkten mit alten Sicherheitsagenten können Sie ganz einfach den neuesten unterstützten Sicherheitsagenten installieren, indem Sie auf die Schaltfläche **Upgrade durchführen** klicken.

> **Beachten Sie**
> Dieser Bericht steht nur zur Verfügung, wenn ein Upgrade für die GravityZone-Lösung durchgeführt wurde.

Ransomware-Aktivität

Informiert Sie über die Ransomware-Angriffe, die GravityZone auf den von Ihnen verwalteten Endpunkten erkannt hat, und stellt Ihnen die erforderlichen Tools zur Verfügung, um die von den Angriffen betroffenen Dateien wiederherzustellen.

Anders als andere Berichte ist der Bericht als eigene Seite im Control Center verfügbar und kann direkt über das GravityZone-Hauptmenü aufgerufen werden.

Die Seite **Ransomware-Aktivität** besteht aus einem Raster, das für jeden Ransomware-Angriff folgende Informationen anzeigt:

- Name, IP-Adresse und FQDN des Endpunkts, auf dem der Angriff stattfand

- Das Unternehmen, zu dem der Endpunkt gehört
- Der Name des Benutzers, der während des Angriffs angemeldet war
- Der Angriffstyp, d. h. lokal oder remote
- Der Prozess, unter dem die Ransomware bei lokalen Angriffen ausgeführt wurde bzw. die IP-Adresse, von der aus der Angriff bei Remote-Angriffen gestartet wurde
- Datum und Uhrzeit des Fundes
- Anzahl der Dateien, die verschlüsselt wurden, bis der Angriff blockiert wurde
- Der Status der Wiederherstellungsaktion für alle Dateien auf dem Zielendpunkt

Einige Details werden standardmäßig ausgeblendet. Klicken Sie auf die Schaltfläche **Spalten ein-/ausblenden** oben rechts auf der Seite, um die Details zu konfigurieren, die Sie im Raster anzeigen möchten. Wenn Sie viele Einträge im Raster haben, können Sie Filter über die Schaltfläche **Filter ein-/ausblenden** oben rechts auf der Seite ausblenden.

Weitere Informationen erhalten Sie durch Anklicken der Anzahl der Dateien. Sie können eine Liste mit dem vollständigen Pfad zu den ursprünglichen und wiederhergestellten Dateien sowie den Wiederherstellungsstatus für alle an dem ausgewählten Ransomware-Angriff beteiligten Dateien anzeigen.

Wichtig
Die Sicherungskopien sind maximal 30 Tage lang verfügbar. Bitte achten Sie auf das Datum und die Uhrzeit, zu denen die Dateien noch wiederhergestellt werden können.

So können Sie von Ransomware betroffenen Dateien wieder herstellen:

1. Wählen Sie die Angriffe aus, die im Raster aufgeführt werden sollen.
2. Klicken Sie auf **Dateien wiederherstellen**. Ein Bestätigungsfenster wird angezeigt.

   Es wird eine Wiederherstellungsaufgabe erstellt. Sie können ihren Status wie bei jeder anderen Aufgabe in GravityZone auf der Seite **Aufgaben** einsehen.

Wenn Funde das Ergebnis harmloser Prozesse sind, gehen Sie wie folgt vor:

1. Wählen Sie die Datensätze im Raster aus.

2. Klicken Sie auf die Schaltfläche **Ausschluss hinzufügen**.
3. Wählen Sie im neuen Fenster die Richtlinien aus, für die der Ausschluss gelten soll.
4. Klicken Sie auf **Hinzufügen**.

   wird alle möglichen Ausschlüsse anwenden: auf den Ordner, auf den Prozess und auf die IP-Adresse.

   Sie können sie im Richtlinienabschnitt **Malware-Schutz > Einstellungen > Benutzerdefinierte Ausschlüsse** überprüfen oder anpassen.

Beachten Sie
Ransomware-Aktivität zeichnet Ereignisse zwei Jahre lange auf.

8.1.2. Exchange-Server-Berichte

Die folgenden Arten von Berichten sind für Exchange-Server verfügbar:

Exchange - Blockierte Inhalte und Anhänge
Enthält Informationen über E-Mails oder Anhänge, die von der Inhaltssteuerung während eines bestimmten Zeitraums von den ausgewählten Servern gelöscht wurden. Angezeigt wird:

- E-Mail-Adressen des Absenders und der Empfänger.

  Wenn die E-Mail mehrere Empfänger hat, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.
- E-Mail-Betreff.
- Erkennungstyp; zeigt an, von welchem Inhaltssteuerungsfilter die Bedrohung gefunden wurde.
- Die durchgeführte Aktion.
- Der Server, auf dem die Bedrohung gefunden wurde.

Exchange – blockierte unscannbare Anhänge
Enthält Informationen zu E-Mails mit nicht scanbaren Anhängen (überkomprimiert, passwortgeschützt usw.), die auf den ausgewählten Exchange-Mail-Servern über einen bestimmten Zeitraum blockiert wurden. Die Informationen beziehen sich auf:

- E-Mail-Adressen des Absenders und der Empfänger.

Wenn die E-Mail an mehrere Empfänger gesendet wurde, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.

- E-Mail-Betreff.
- Zur Entfernung von nicht scanbaren Anhängen durchgeführte Aktionen:
  - **Gelöschte E-Mail** zeigt an, dass die gesamte E-Mail entfernt wurde.
  - **Gelöschte Anhänge** allgemeine Bezeichnung für alle Aktionen, bei denen Anhänge aus einer E-Mail-Nachricht entfernt werden, so zum Beispiel durch Löschen des Anhangs, durch Verschieben in die Quarantäne oder durch Austausch mit einer Benachrichtigung.

  Mit einem Klick auf den Link in der Spalte **Aktion** können Sie Details zu jedem blockierten Anhang und die jeweils durchgeführte Aktion anzeigen.
- Zeitpunkt des Fundes.
- Der Server, auf dem die E-Mail gefunden wurde.

Exchange - E-Mail-Scan-Aktivität

Zeigt Statistiken zu den vom Exchange-Schutz-Modul während eines bestimmten Zeitraums durchgeführten Aktionen an.

Die Aktionen werden nach Typ (Malware, Spam, unzulässiger Anhang und unzulässiger Inhalt) und nach Server zu Gruppen zusammengefasst.

Die Statistiken beziehen sich auf die folgenden E-Mail-Status:

- **In Quarantäne.** Diese E-Mails wurden in den Quarantäne-Ordner verschoben.
- **Gelöscht/Abgelehnt.** Diese E-Mails wurden vom Server gelöscht oder abgelehnt.
- **Umgeleitet.** Diese E-Mails wurden an die in der Richtlinie angegebene E-Mail-Adresse umgeleitet.
- **Bereinigt und zugestellt.** Diese E-Mails wurden von den Filtern durchgelassen, nachdem Bedrohungen entfernt worden sind.

  Eine E-Mail gilt als bereinigt, wenn alle als potenziell schädlich erkannten Anhänge desinfiziert, in die Quarantäne verschoben, gelöscht oder durch Text ersetzt wurden.

- **Geändert und zugestellt.** Diese E-Mails wurden von den Filtern durchgelassen, nach dem Scan-Informationen den E-Mail-Headern hinzugefügt wurden.
- **Ohne weitere Aktion zugestellt.** Diese E-Mails wurden vom Exchange-Schutz ignoriert und von den Filtern durchgelassen.

Exchange - Malware-Aktivität

Enthält Informationen über E-Mails mit Malware-Bedrohungen, die in einem bestimmten Zeitraum auf den ausgewählten Exchange-Mail-Servern gefunden wurden. Die Informationen beziehen sich auf:

- E-Mail-Adressen des Absenders und der Empfänger.

  Wenn die E-Mail an mehrere Empfänger gesendet wurde, zeigt der Bericht statt der E-Mail-Adressen die Anzahl der Empfänger mit einem Link an, der ein Fenster mit der Liste der E-Mail-Adressen öffnet.
- E-Mail-Betreff.
- E-Mail-Status nach Malware-Scan.

  Mit einem Klick auf den Status-Link werden Details zur gefundenen Malware und der durchgeführten Aktion angezeigt.
- Zeitpunkt des Fundes.
- Der Server, auf dem die Bedrohung gefunden wurde.

Exchange - Top-10 der gefundenen Malware

Zeigt die 10 am häufigsten in E-Mail-Anhängen gefundenen Malware-Bedrohungen. Sie können zwei verschiedene Ansichten mit unterschiedlichen Statistiken generieren. Die eine zeigt die Anzahl der Funde nach betroffenen Empfängern, die andere nach Absendern an.

Nehmen wir an, GravityZone hat eine E-Mail mit infiziertem Anhang gefunden, die an fünf Empfänger gesendet wurde.

- In der Empfängeransicht:
  - Der Bericht zeigt fünf Funde.
  - In den Berichtdetails werden nur die Empfänger, nicht die Absender, angezeigt.
- In der Absenderansicht:
  - Der Bericht zeigt einen Fund.

– In den Berichtdetails wird nur der Absender, nicht die Empfänger, angezeigt.

Außer dem Namen der Malware und dem des Absenders/Empfängers enthält der Bericht die folgenden Informationen:

- Malware-Typ (Virus, Spyware, PUA, usw.)
- Der Server, auf dem die Bedrohung gefunden wurde.
- Maßnahmen, die das Malware-Schutz-Modul ergriffen hat.
- Zeitpunkt des letzten Fundes.

Exchange - Top-10 der Malware-Empfänger

Zeigt die 10 E-Mail-Empfänger an, die während eines bestimmten Zeitraums am häufigsten das Ziel von Malware waren.

In den Berichtdetails wird die gesamte Liste der Malware aufgeführt, die diese Empfänger betraf, zusammen mit den durchgeführten Aktionen.

Exchange - Top-10 der Spam-Empfänger

Zeigt die 10 E-Mail-Empfänger an, die in einem bestimmten Zeitraum die meisten erkannten Spam- oder Phishing-E-Mails empfangen haben. Im Bericht werden auch die Aktionen aufgeführt, die für diese E-Mails durchgeführt wurden.

8.2. Berichte erstellen

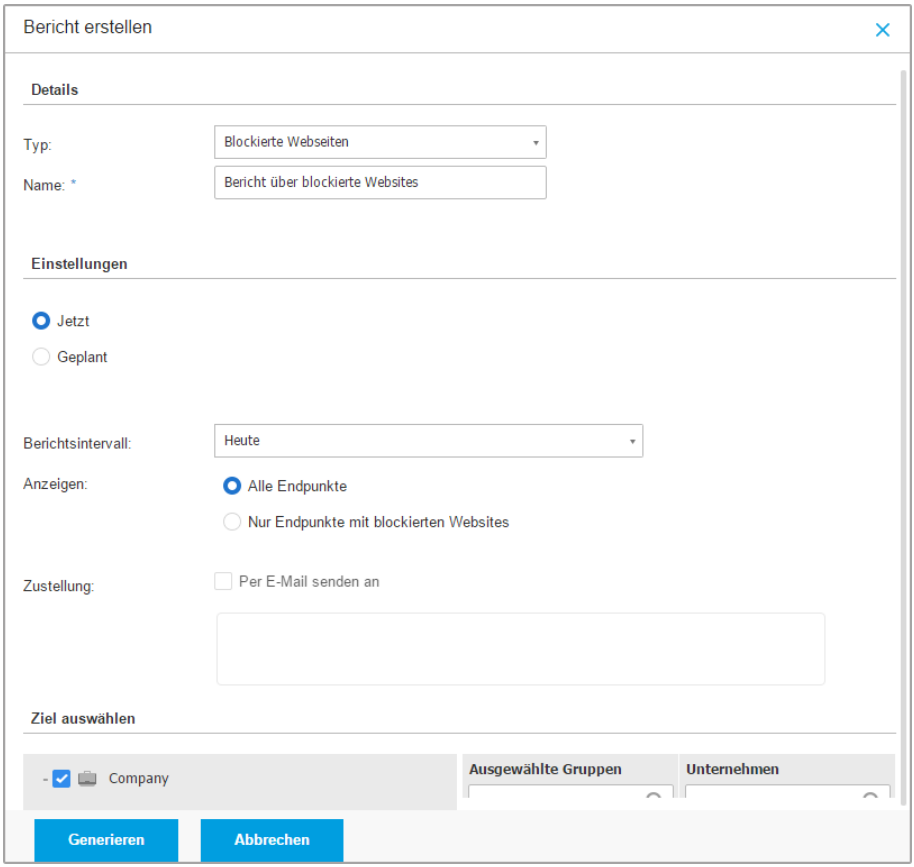
Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **Sofortberichte.** Sofortberichte werden automatisch angezeigt, sobald sie erstellt wurden.
- **Geplante Berichte.** Berichte können so geplant werden, dass sie in regelmäßigen Abständen und/oder zu einem bestimmten Zeitpunkt erstellt werden. Eine Liste aller geplanten Berichte finden Sie auf der Seite **Berichte**.

Wichtig
Sofortberichte werden automatisch gelöscht, wenn Sie die Berichtsseite schließen. Geplante Berichte werden auf der Seite **Berichte** gespeichert und angezeigt.

Um einen Bericht zu erstellen:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.



Berichtsoptionen

3. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus. Weitere Informationen finden Sie unter „Berichtstypen“ (S. 104)
4. Geben Sie einen eindeutigen Namen für den Bericht ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen.
5. Konfigurieren Sie die Wiederholung des Berichts:
   - Mit **Jetzt** erstellen Sie einen Sofortbericht.

- Mit **Geplant** können Sie den Bericht so konfigurieren, dass er regelmäßig nach einem gewünschten Intervall generiert wird:
  - Stündlich. Immer nach einer festgelegten Anzahl von Stunden.
  - Täglich. Hierbei können Sie auch die Startzeit (Stunde und Minute) festlegen.
  - Wöchentlich, am festgelegten Wochentag zur festgelegten Startzeit (Stunde und Minute).
  - Monatlich, am festgelegten Tag des Monats zur festgelegten Startzeit (Stunde und Minute).

6. Für die meisten Berichtstypen müssen Sie das Intervall angeben, auf das sich die im Bericht enthaltenen Daten beziehen. Der Bericht zeigt nur Daten aus dem gewählten Zeitraum an.
7. Viele Berichtsarten enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Verwenden Sie die Filtermöglichkeiten im Bereich **Anzeigen**, um nur die gewünschten Informationen abzurufen.

   Für einen **Update-Status**-Bericht können Sie zum Beispiel auf Wunsch nur die Netzwerkobjekte anzeigen, die nicht aktualisiert wurden, oder diejenigen, die neu gestartet werden müssen, um das Update abzuschließen.
8. **Zustellung**. Um einen geplanten Bericht als E-Mail geschickt zu bekommen, markieren Sie das entsprechende Kästchen. Geben Sie die gewünschten E-Mail-Adresse in das Feld darunter ein. Die E-Mail enthält standardmäßig ein Archiv mit beiden Berichtdateien (PDF und CSV). Über die Kästchen im Bereich **Dateien anhängen** können Sie festlegen, welche Dateien per E-Mail versandt werden sollen und wie.
9. **Ziel auswählen**. Scrollen Sie nach unten, das Ziel des Berichts zu konfigurieren. Wählen Sie eine oder mehrere Gruppen von Endpunkten, die Sie in den Bericht einbeziehen möchten.
10. Klicken Sie je nach Wiederholungsintervall auf **Generieren**, um einen Sofortbericht zu erstellen, oder auf **Speichern**, um einen geplanten Bericht zu erstellen.
    - Ein Sofortbericht wird sofort angezeigt, nachdem Sie auf **Generieren** klicken. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von

der Anzahl der verwalteten Netzwerkobjekte ab. Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.

- Der geplante Bericht wird in der Liste auf der Seite **Berichte** angezeigt. Nachdem eine Berichtsinstanz generiert wurde, können Sie den Bericht anzeigen, indem Sie auf den entsprechenden Link in der Spalte **Bericht anzeigen** auf der Seite **Berichte** klicken.

8.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.

Die Berichteseite

Alle geplanten Berichte werden zusammen mit nützlichen Informationen zu den Berichten in einer Tabelle angezeigt:

- Name und Art des Berichts
- Berichtwiederholung
- Zuletzt generierte Instanz

Beachten Sie
Geplante Berichte sind nur für den Benutzer verfügbar, der diese auch erstellt hat.

Um Berichte nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Sie können das Suchfeld leeren, indem Sie mit dem Mauszeiger darüber fahren und auf das × **Löschen**Symbol klicken.

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

8.3.1. Berichte betrachten

So zeigen Sie einen Bericht an:

1. Gehen Sie zur Seite **Berichte**.

2. Sortieren Sie die Berichte nach Namen, Typ oder Wiederholung, um den gewünschten Bericht leichter zu finden.
3. Klicken Sie in der Spalte **Bericht anschauen** auf den entsprechenden Link, um den Bericht anzuzeigen. Die jüngste Berichtsinstanz wird angezeigt.

   Wie Sie alle Instanzen eines Berichts anzeigen, erfahren Sie unter„Berichte speichern“ (S. 127)

Alle Berichte haben eine Zusammenfassungsteil (die obere Hälfte der Berichtsseite) und einen Detailsteil (die untere Hälfte der Berichtsseite).

- Der Zusammenfassungsbereich enthält statistische Daten (Kuchendiagramme und Grafiken) für alle Netzwerkobjekte sowie allgemeine Informationen über den Bericht wie den Berichtszeitraum (sofern anwendbar), Berichtsziel, usw.
- Der Detailbereich enthält Informationen zu allen entsprechenden Netzwerkobjekten.

Beachten Sie

- Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden.
- Klicken Sie auf den Bereich der Grafik (Kuchensegment oder Balken), der Sie interessiert, um in der Tabelle Details dazu anzuzeigen.

8.3.2. Geplante Berichte bearbeiten

Beachten Sie
Wenn Sie einen geplanten Bericht bearbeiten, werden sämtliche Änderungen mit der nächsten Ausführung des Berichts wirksam. Zuvor erstellte Berichte sind von den Änderungen nicht betroffen.

Um die Einstellungen eines geplanten Berichts zu ändern:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf den Berichtnamen.
3. Ändern Sie die Berichtseinstellungen nach Bedarf. Sie können die folgenden Änderungen vornehmen:
   - **Berichtsname.** Geben Sie dem Bericht einen eindeutigen Namen, der seinen Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie

den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen. Berichte die anhand eines geplanten Berichts erstellt werden, erhalten auch den entsprechenden Namen.

- **Berichtswiederholung (geplant).** Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
- **Einstellungen**
  - Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
  - Der Bericht wird nur Daten aus dem ausgewählten Intervall enthalten. Sie können das Intervall ab der nächsten Ausführung ändern.
  - Die meisten Berichte enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Wenn Sie den Bericht in der Konsole anzeigen, sind unabhängig von den gewählten Optionen immer alle Informationen verfügbar. Wenn Sie den Bericht herunterladen oder per E-Mail versenden, werden nur die Berichtszusammenfassung und die ausgewählten Informationen in der PDF-Datei enthalten sein. Die Berichtsdetails sind nur im CSV-Format verfügbar.
  - Sie können den Bericht auch per E-Mail erhalten.
- **Ziel wählen.** Die ausgewählte Option weist auf die Art des aktuellen Berichtsziels hin (entweder Gruppen oder einzelne Netzwerkobjekte). Klicken Sie auf den entsprechenden Link, um das aktuelle Berichtsziel anzuzeigen. Sie können das Berichtsziel ändern, indem Sie die Gruppen oder Netzwerkobjekte auswählen, die in dem Bericht eingeschlossen werden sollen.

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

8.3.3. Geplante Berichte löschen

Wenn ein geplanter Bericht nicht mehr benötigt wird, empfiehlt es sich, diesen zu löschen. Durch das Löschen eines geplanten Berichts werden alle Instanzen, die dieser bis zu diesem Zeitpunkt automatisch erstellt hat, gelöscht.

Um einen geplanten Bericht zu löschen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

8.4. Berichte speichern

Standardmäßig werden geplante Berichte automatisch im Control Center gespeichert.

Wenn Sie Berichte über einen längeren Zeitraum hin benötigen, können Sie sie auf Ihrem Computer abspeichern. Die Zusammenfassung des Berichts ist im PDF-Format verfügbar; die Berichtsdetails sind jedoch nur im CSV-Format verfügbar.

Sie können Berichte auf zweierlei Weise speichern:

- Exportieren
- Download

8.4.1. Berichte exportieren

So exportieren Sie den Bericht auf Ihren Computer:

1. Klicken Sie je nach gewünschtem Format auf **CSV exportieren** oder **PDF exportieren**.
2. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

8.4.2. Berichte herunterladen

Einen Berichtsarchiv enthält sowohl die Zusammenfassung als auch die Details eines Berichts.

So laden Sie ein Berichtsarchiv herunter:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, den Sie speichern möchten.
3. Klicken Sie auf die Schaltfläche **Herunterladen** und wählen Sie entweder **Letzte Instanz**, um die zuletzt erstellte Instanz des Berichts herunterzuladen, oder **Vollständiges Archiv**, um ein Archiv herunterzuladen, das sämtliche Instanzen enthält.

   Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

8.5. Berichte per E-Mail versenden

Sie können Berichte mit den folgenden Optionen per E-Mail versenden:

1. Wenn Sie den angezeigten Bericht direkt per E-Mail versenden möchten, klicken Sie auf die Schaltfläche **E-Mail**. Der Bericht wird an die mit Ihrem Konto verknüpfte E-Mail-Adresse gesendet.
2. So konfigurieren Sie den Versand geplanter Berichte per E-Mail:
   a. Gehen Sie zur Seite **Berichte**.
   b. Klicken Sie auf den gewünschten Berichtnamen.
   c. Unter **Einstellungen > Zustellung Per Email senden an** auswählen.
   d. Geben Sie die gewünschte E-Mail-Adresse im Feld darunter ein. Sie können beliebig viele E-Mail-Adressen hinzufügen.
   e. Klicken Sie auf **Speichern**.

> **Beachten Sie**
> In der PDF-Datei, die per E-Mail gesendet wird, sind nur die Berichtszusammenfassung und das Diagramm enthalten. Die Berichtsdetails sind in der CSV-Datei enthalten.

Berichte werden als ZIP-Archive per E-Mail gesendet.

8.6. Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen. Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

9. BENUTZERAKTIVITÄTSPROTOKOLL

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Die Benutzeraktivitätsliste enthält je nach Ihren Administratorrechten die folgenden Ereignisse:

- Anmelden und Abmelden
- Berichte erstellen, bearbeiten, umbenennen und löschen
- Dashboard-Portlets hinzufügen und entfernen
- Problembehandlungsvorgänge auf betroffenen Maschinen starten, beenden, abbrechen und anhalten
- Bearbeiten der Authentifizierungseinstellungen für die GravityZone-Benutzerkonten.

Die Seite Benutzeraktivität

Um aufgezeichnete Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie eine Suche definieren. Geben Sie die Suchkriterien in die verfügbaren Felder ein und klicken Sie auf **Suchen**. Alle zu Ihren Kriterien passenden Einträge werden in der Tabelle angezeigt.

Die Spalten geben nützliche Informationen zu den aufgelisteten Ereignissen:

- Der Name des Benutzers, der die Aktion durchgeführt hat.
- Benutzerrolle.
- Aktion, die das Ereignis ausgelöst hat.
- Art des Konsolenobjekts, das von der Aktion betroffen ist.
- Bestimmtes Konsolenobjekt, das von der Aktion betroffen ist.
- Zeitpunkt, zu dem das Ereignis eingetreten ist.

Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierungsreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

10. HILFE ERHALTEN

Sollten Probleme oder Fragen im Zusammenhang mit GravityZone auftreten, wenden Sie sich bitte an einen Administrator.

10.1. 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.

10.2. Hilfe anfordern

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

A. Anhänge

A.1. Sandbox Analyzer-Objekte

A.1.1. 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.1.2. 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.1.3. Standardausschlüsse bei automatischer Übermittlung

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

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Boot-Sektor:

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootkit

Ein Bootkit ist ein Schadprogramm, das den Master Boot Record (MBR), den Volume Boot Record oder den Boot-Sektor infizieren kann. Ein Bootkit bleibt auch nach einem Neustart des Systems aktiv.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen
Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können.

Ereignisanzeige
Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Exploit
Als Exploit wird zum einen eine Methode bezeichnet, mit der Unbefugte auf einen Computer zugreifen, zum anderen eine Schwachstelle in einem System, über die das System angegriffen werden kann.

Fehlalarm
Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Gezielte Angriffe
Cyber-Angriffe, die es hauptsächlich auf finanzielle Vorteile oder die Erschütterung eines guten Rufs abgesehen haben. Opfer können Einzelpersonen, Unternehmen, eine Software oder ein System sein. In jedem Fall wird das Opfer vor dem Angriff genauestens studiert. Diese Art von Angriffen wird über einen langen Zeitraum hinweg und in verschiedenen Phasen durchgeführt, wobei oft mehr als ein Einfallstor ausgenutzt wird. Sie werden kaum bemerkt, und wenn doch, dann meist erst, wenn es schon zu spät ist.

Grayware
Eine Klasse von Software-Anwendungen irgendwo zwischen legitimer Software und Malware. Sie ist zwar nicht so unmittelbar schädlich wie Malware, die die Systemfunktion direkt beeinträchtigt, ihr Verhalten ist aber dennoch beunruhigend und kann zu unerwünschten Situationen führen. Daten können gestohlen, Identitäten missbraucht und Werbung eingeblendet werden. Die verbreitesten Arten von Grayware sind Spyware und Adware.

Heuristik
Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden

kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Malware-Scan-Ressourcenkonflikt

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet. Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.

Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Passwort-Stehler

Ein Passwort-Stehler sammelt Daten wie Benutzernamen und Passwörter für Konten. Die gestohlenen Zugangsdaten werden dann zu kriminellen Zwecken genutzt.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum

Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Ransomware

Eine Schadsoftware, die Ihren Computer sperrt oder Ihnen den Zugriff auf Ihre Dateien und Anwendungen verwehrt. Ransomware verlangt die Zahlung eines bestimmten Betrags (Lösegeldzahlung) als Gegenleistung für einen Entschlüsselungscode, der den Zugang zum Computer und Ihren Dateien wieder freigibt.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Schutzebenen

GravityZone bietet Schutz durch eine Reihe von Modulen und Rollen, die gemeinsam als Sicherheitsebenen bezeichnet werden und in Endpunktschutz (EPP) bzw. Kernschutz sowie verschiedene Add-ons unterteilt sind. Der Endpunktschutz umfasst Malware-Schutz, Advanced Threat Control, Erweiterter Exploit-Schutz, Firewall, Inhaltssteuerung, Gerätesteuerung, Network Attack Defense, Power-User und Relais. Die Add-ons umfassen Sicherheitsebenen wie Security for Exchange und Sandbox Analyzer.

Weitere Einzelheiten zu den mit Ihrer GravityZone-Lösung erhältlichen Sicherheitsebenen finden Sie unter „GravityZone-Sicherheitsebenen“ (S. 2).

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen

über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht

hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Verdächtige Dateien und Netzwerkverkehr

Verdächtige Dateien sind solche mit einer zweifelhaften Reputation. Diese Einstufung basiert auf mehreren Faktoren, darunter: Vorhandensein der digitalen Signatur, Anzahl der Vorkommen in Computernetzwerken, verwendeter Packer, usw. Netzwerkverkehr gilt als verdächtig, wenn er vom Muster abweicht. Zum Beispiel bei unzuverlässiger Quelle, Verbindungsanfragen an ungewöhnliche Ports, hohe Bandbreitennutzung, zufällig scheinende Verbindungszeiten, usw.

Windows-Downloader

Es ist ein generischer Name für ein Programm, dessen primäre Funktion darin besteht, Inhalte zu unerwünschten oder schädlichen Zwecken herunterzuladen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.