Bitdefender GravityZone Ultra Suite

AGILITÄT UND PRÄZISION ZUR AUFDECKUNG UND ABWEHR AUCH SCHWER GREIFBARER BEDROHUNGEN

GravityZone Ultra mit Endpoint Security XDR überzeugt besonders dort, wo Pure-Play-EDR-Produkte viel zu komplex und aufwendig sind. Dabei sorgt es reibungslos für Prävention, Erkennung und Unschädlichmachung von komplexen Angriffen, gegen den herkömmlicher Malware-Schutz keine Chance hat. In nur einer einzigen einheitlichen Sicherheitssuite sorgt GravityZone Ultra für:

- Reduzierung der Angriffsfläche (dank Firewall, Anwendungssteuerung, Inhaltssteuerung und Patch-Verwaltung)
- Datenschutz (dank vollständiger Festplattenverschlüsselung)
- Erkennung schon vor Ausführung und Beseitigung von Malware (dank optimierbarem machine Learning, Prozessprüfung in Echtzeit und Sandbox-Analysen)
- Automatische Erkennung, einfache Untersuchung und Vor-Ort-Bereinigung über die neu eingeführte Möglichkeit zur Endpunkt-Ereignisaufzeichung und Bedrohungsanalyse in Endpoint Security XDR

Dies ermöglicht nahtlose Bedrohungsprävention, zuverlässige Vorfallerkennung und intelligente Reaktionen zur Minimierung des Infektionsrisikos und Verhinderung von Sicherheitsverletzungen.

Als integrierte Suite für den Endpunktschutz sorgt GravityZone Ultra für gleichbleibend hohe Sicherheit in der gesamten IT-Umgebung. Für Angreifer bieten sich keine unzureichend geschützten Endpunkte, die als Ausgangspunkt für böswillige Aktionen gegen das Unternehmen dienen können. GravityZone Ultra basiert auf einer einfachen, integrierten Architektur mit zentraler, einheitlicher Verwaltung für Endpunkte und Rechenzentren gleichermaßen. So können Unternehmen den Endpunktschutz schnell bereitstellen und nach der Implementierung den Verwaltungsaufwand reduzieren.

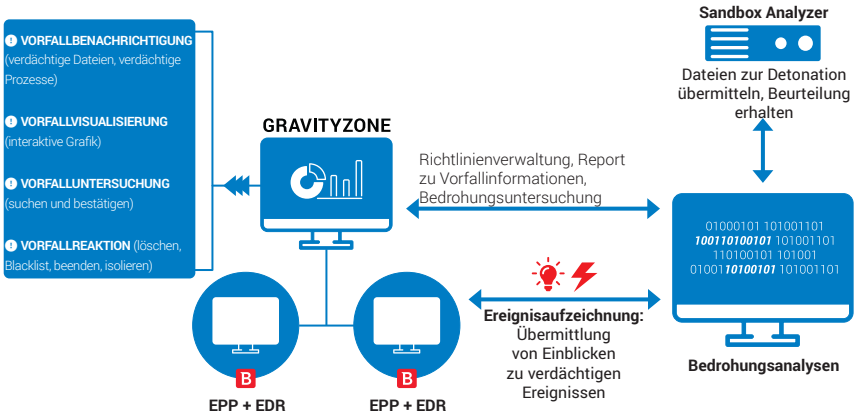


Abbildung 1. Bitdefender XDR: Prävention, Erkennung und Reaktion mit nur einem Agenten, verwaltet über die GravityZone-Konsole

EDR leicht gemacht

Durch die Sichtbarmachung möglicher Kompromittierungen (Indicators of Compromise), die Ein-Klick-Bedrohungsuntersuchung und die Workflows zur Reaktion auf Sicherheitsvorfälle erfordert GravityZone Ultra weniger Ressourcen und Fachwissen zur Aufrechterhaltung des Sicherheitsbetriebs. Die neue Möglichkeit zur Endpunktdatenaufzeichnung ist eine nahtlose Ergänzung des bestehenden Sicherheitsmechanismen und protokolliert ein breites Spektrum an Systemaktivitäten (Datei- & Prozesserstellung, Programminstallationen, Laden von Modulen, Registry-Änderungen, Netzwerkverbindungen uvm.) zur Unterstützung der unternehmensweiten Sichtbarmachung von Ereignisketten im Zuge eines Angriffs.

Das Modul für die Bedrohungsanalyse läuft in der Cloud und durchsucht ununterbrochen Verhaltensereignisse in den Systemaktivitäten und erstellt einer priorisierte Liste der Vorfälle für die weitere Untersuchung und Reaktion.

Hauptvorteile

Endpoint Security XDR geht weit über herkömmliche Endpunktschutzfunktionen hinaus und gibt Sicherheitsanalysten und Vorfallreaktionsteams die Werkzeuge an die Hand, die sie zur Analyse verdächtiger Aktivitäten und zur Untersuchung komplexer Bedrohungen benötigen:

- Echtzeiteinblicke in die Endpunkte
- Offenlegung verdächtiger Aktivitäten
- Ein-Klick-Untersuchungen
- Alarmeinschätzung und Visualisierung der Vorfallanalyse
- Verfolgung von laufenden Angriffen und seitlichen Bewegungen
- Schnelle Abhilfe
- Schnelle Auflösung, Eindämmung und Bereinigung reduziert Verweilzeiten

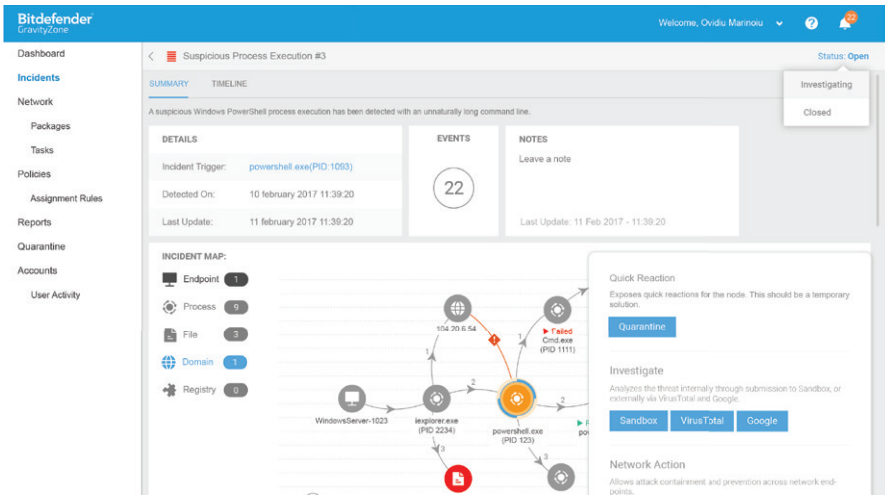


Abbildung 2. Auf der Vorfalldetailseite findet sich eine übersichtliche Aufstellung und Protokollierung der Vorfälle. So kann das Fachpersonal bequem sachdienliche Hinweise sammeln und angemessen reagieren.

Bessere Einblicke in die Sicherheitslage. Vermeidung übermäßiger Fehlalarme.

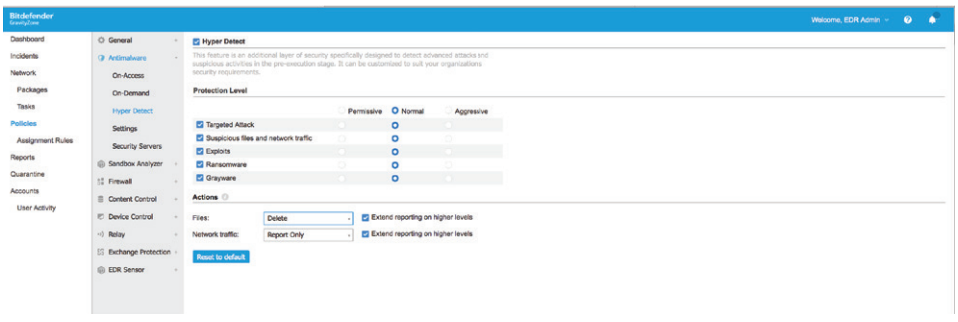
Nur relevante, korrelierte und nach Schwere bewertete Ereignisse werden zur manuellen Analyse und Behebung vorgelegt. Störungen und redundante Informationen werden auf ein Minimum reduziert, da die Mehrzahl der Angriffe und komplexen Angriffe schon vor oder während der Ausführung blockiert werden. Schwer greifbare Bedrohungen, so auch dateilose Malware, Exploits, Ransomware und verschleierte Malware, werden durch die hochwirksamen und mehrstufigen Next-Generation-Präventsionstechnologien und die verhaltensbasierte Prozessprüfung bei Ausführung neutralisiert. Automatische Reaktionen und Reparaturen machen menschliches Eingreifen bei blockierten Angriffen unnötig.

Durch die hochpräzise Erkennung können sich Sicherheitsteams auf echte Vorfälle und Bedrohungen konzentrieren:

- Keine Ablenkungen und Störungen durch ständige Fehlalarme
- Effektive Bedrohungsprävention sorgt für weniger Vorfälle
- Die manuelle Bereinigung blockierter Angriffe entfällt dank automatischer Bereinigung und Reparatur

Intelligente Reaktionen für noch zuverlässigere Prävention

GravityZone Ultra ist eine integrierte Lösung, die Prävention, Erkennung und Reaktion in sich vereint. So kann eine schnelle Reaktion und Wiederherstellung von Endpunkten gewährleistet werden, die sie sogar noch sicherer machen. Unter Einsatz der auf den Endpunkten während der Prüfung gesammelten Bedrohungserkenntnisse können in der zentralen Oberfläche Richtlinien sofort entsprechend angepasst und Sicherheitslücken zur Vermeidung zukünftiger Vorfälle geschlossen werden. So wird die Sicherheit der gesamten Umgebung verbessert.



Umfassende Plattform für die Endpunktsicherheit mit nur einem Agenten und einer Konsole

GravityZone Ultra bietet alle Möglichkeiten zur Absicherung und Next-Generation-Prävention, die Sie schon aus Endpoint Security HD und der GravityZone-Elite-Suite kennen:

- Risikominimierung durch starke Prävention
- Die Erkennung auf Grundlage von maschinellem Lernen und Verhaltensüberwachung wehrt auch unbekannte Bedrohungen schon vor und während der Ausführung ab
- Erkennung und Blockierung von skriptbasierter, dateiloser, schwer aufzuspürender und speziell angepasster Malware mit automatischer Bereinigung
- Speicherschutz zur Abwehr von Exploits
- Reduzierte Angriffsfläche durch IT-Sicherheitssteuerung
- Integrierte Client-Firewall, Gerätesteuerung, Filter für Webinhalte, Anwendungssteuerung, Patch-Management und vieles mehr.

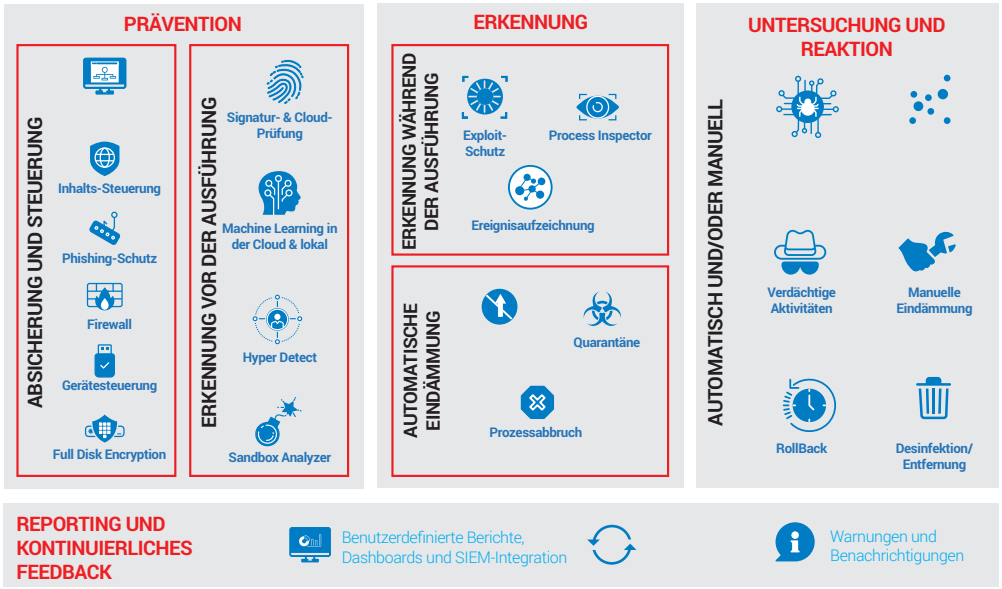
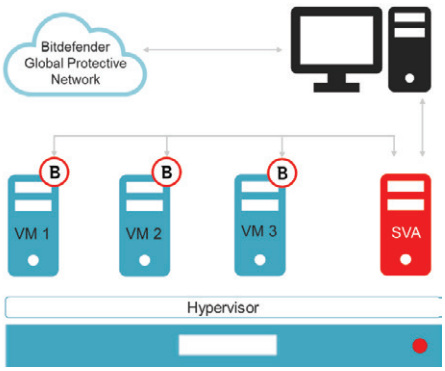


Abbildung 3. Bitdefender XDR: Die umfassende Plattform für die Endpunktsicherheit

Für ein sicheres Rechenzentrum

Mit Security for Virtualized Environments (SVE) bietet die GravityZone-Elite-Suite eine Schutzkomponente speziell für Rechenzentren, die nahtlos mit Bitdefender Endpoint Security XDR integriert ist. Beim Malware-Schutz auf virtualisierten Maschinen ungeschlagen, sorgt diese Sicherheitslösung speziell für virtualisierte Rechenzentren nicht nur für optimale Konsolidierungsraten, sondern auch für reduzierte Betriebskosten. GravityZone SVE ist eine Enterprise-Lösung, die eigens für die Anforderungen großer Rechenzentren entwickelt wurde. Die Integration in Produktivumgebungen erfolgt problemlos und die Vorteile dieser Technologie machen sich unabhängig von der Größe der virtuellen Umgebung bemerkbar.

Hauptvorteile



Flexibilität
Mit SVE lässt sich die Sicherheit eines Rechenzentrums sowohl bei der Einrichtung als auch beim täglichen Betrieb über den gesamten Lebenszyklus automatisieren, selbst in hochgradig dynamischen Umgebungen. Es lässt sich mit VMware (vCenter, vShield, NSX), Citrix XenCenter und Nutanix Enterprise Cloud Platform integrieren und lässt sich schnell und automatisiert installieren und einrichten.

Effizienter Betrieb
Das GravityZone Control Center ist die zentrale Schaltstelle, die alles von der Installation über die Verwaltung bis hin zu Upgrades extrem unkompliziert macht und volle Transparenz aller virtuellen und physischen Server und Arbeitsplatzrechner gewährt. Dank der zentralisierten Erstellung und automatischen Anwendung von Sicherheitsrichtlinien wird der IT-Betrieb optimiert und gleichzeitig die Compliance verbessert.

Verbesserte Infrastrukturnutzung
Dank zentralisierter Scans und einem schlanken Agenten werden Festplatten-, Arbeitsspeicher, CPU- und E/A-Anforderungen an Host-Server drastisch gesenkt, was eine höhere VM-Dichte und einen besseren ROI der IT-Infrastruktur beteutet.

Universelle Kompatibilität
Kompatibel mit allen führenden Hypervisor-Plattformen (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM und Nutanix AHV) sowie mit Windows und Linux als Gastbetriebssystem.

Unbegrenzte lineare Skalierbarkeit
Durch den Einsatz mehrerer SVAs kann die Scan-Kapazität erhöht werden, wenn das durch ein Anwachsen des Rechenzentrums oder der Zahl der VMs nötig werden sollte. Wenn eine SVA der Last nicht mehr gerecht wird, können ganz einfach neue hinzugefügt werden. Ein weiterer Vorteil der Bereitstellung mehrerer SVAs liegt in der verbesserten Ausfallsicherheit und Lastverteilung: Die Last fehlerhafter/überlasteter SVAs kann von einer anderen aktiven oder weniger ausgelasteten SVA übernommen werden.

Mehrstufige Sicherheit der nächsten Generation
GravityZone Security for Virtualized Environments umfasst alle essentiellen Sicherheitsschichten von Endpoint Security wie HyperDetect, Sandbox Analyzer und Methoden zur Erkennung dateiloser Angriffe. So bleiben alle im gesamten Rechenzentrum gespeicherten oder verarbeiteten digitalen Unternehmenswerte sicher.

Bestandteile

- Unterstützt die Transformation im Rechenzentrum optimal: SDDC, Hyperkonvergenz und Hybrid Cloud
- Umfassende Integrationen mit VMware, Nutanix, Citrix, AWS und Microsoft für mehr Investitionssicherheit, automatisierte Bereitstellung sowie Inventar- und Lizenzmanagement
- Unterstützung unterschiedlicher Virtualisierungs- und Cloud-Umgebungen über eine einzige Installation
- Eine zentrale Oberfläche für mehr Transparenz und einheitliche Verwaltung über die Hybrid Cloud hinweg.
- Effiziente, ausfallsichere und skalierbare SVA-basierte Architektur, die alle Hypervisoren unterstützt
- Maximale VM-Dichte, kurze Latenzzeiten beim Systemstart und optimale Anwendungsperformance
- Fortschrittliche mehrstufige Sicherheit mit nahtloser Abdeckung überall in der Hybrid Cloud

GravityZone Control Center

GravityZone Control Center ist eine integrierte, zentrale Verwaltungskonsole für sämtliche Sicherheitskomponenten mit denen Endpunkte, Rechenzentren, Exchange-Server und Mobilgeräte geschützt werden. Sie kann in der Cloud gehostet oder lokal installiert werden. In dieser GravityZone-Verwaltungszentrale sind mehrere Rollen zusammengefasst: Datenbank-Server, Kommunikationsserver, Update-Server und Web-Konsole. Das Control Center wird als ein einzelnes Image der virtuellen Appliance ausgeliefert und kann so in nicht einmal 30 Minuten bereitgestellt werden. In größeren Unternehmen kann sie so konfiguriert werden, dass sie mehrere virtuelle Appliances mit mehreren Instanzen bestimmter Rollen und einen integrierten Lastenausgleich verwendet, um Skalierbarkeit und Hochverfügbarkeit sicherzustellen.

Detaillierte Systemanforderungen finden Sie unter www.bitdefender.de/business/ultra-security

BD-NGZ-Nov.23.2017-Tk#: crea2183
Bitdefender-NGZ-UltraSuite-Datasheet-creat2199-A4-de_DE