

GravityZone Ultra Suite

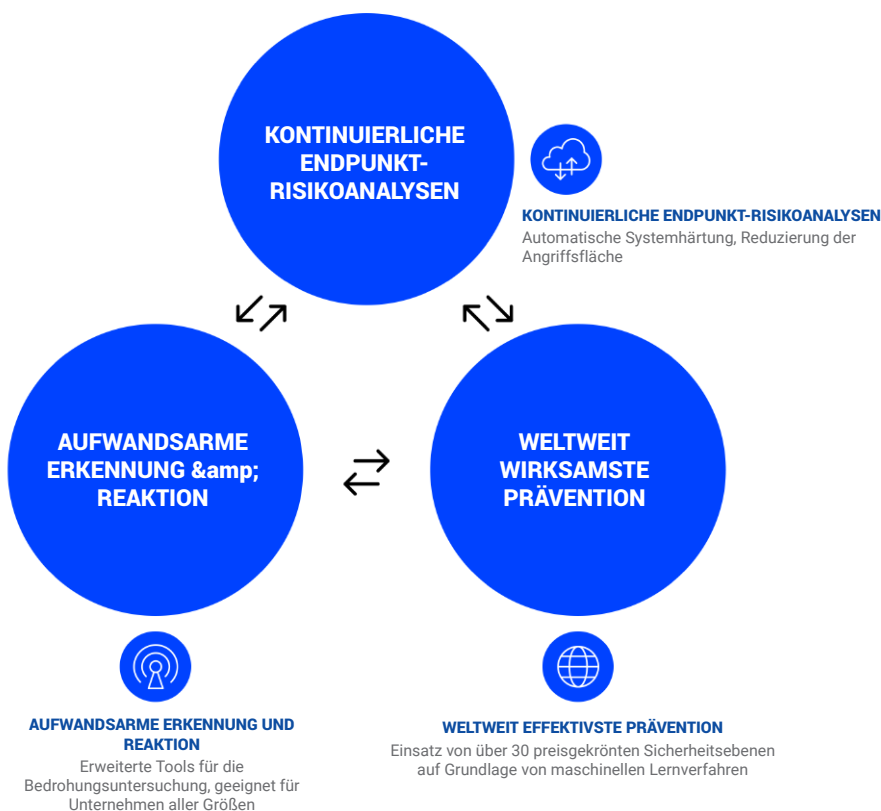
Prävention, Erkennung, Reaktion und Risikoanalysen aus einer Hand

GravityZone Ultra umfasst mehr als 30 Schutzebenen und ist damit die erste Lösung, die unerreicht wirksamen Schutz mit aufwandsarmer EDR und Risikoanalysen für Endpunkte und Benutzerverhalten in einer Architektur mit nur einem Agenten und einer zentralen Konsole vereint.

So wird die Angriffsfläche auf Endpunkten nachhaltig reduziert: Unternehmen jeder Größe können so Sicherheitsverletzungen zuverlässig vermeiden, ihr Sicherheitsmanagement vereinfachen und die Kosten für den Sicherheitsbetrieb erheblich senken.

Mit GravityZone Ultra erhalten Sie:

- **Den weltweit effektivsten Endpunktschutz**, der in unabhängigen Präventionstests regelmäßig den Spitzenplatz belegt
- **Aufwandsarme Endpoint Detection and Response**, dies es jeder IT-Organisation ermöglicht, EDR einzuführen, schnellere Reaktionszeiten zu gewährleisten und Personalkosten für EDR einzusparen
- **Integrierte Risikoanalysen für Endpunkte und Benutzerverhalten**, die Ihre Endpunkte ununterbrochen auf Fehlkonfigurationen überprüfen und Empfehlungen zur Reduzierung der Angriffsfläche geben
- **Einen Agenten und eine Konsole** für alle Funktionen einschließlich Patch Management, Firewall, Verschlüsselung, Anwendungssteuerung, Inhaltssteuerung und vieles mehr
- Optionale Add-on-Module für **Patch Management**, **erweiterte , E-Mail-Sicherheit** und **Datenschutz** für die Optimierung von Sicherheitsprozessen und eine schnellere Reaktion auf Vorfälle



Der weltweit effektivste Endpunktschutz

Für eine lückenlose Bedrohungsabwehr

Mehr als 30 Schutztechnologien, die über mehr als 18 Jahre hinweg von Bitdefenders Sicherheitsforschern, Mathematikern und Datenwissenschaftlern entwickelt wurden, gewährleisten erstklassigen Schutz, der heute in über 38 % aller IT-Sicherheitsprodukte zum Einsatz kommt.

- **Lokales und Cloud-basiertes maschinelles Lernen:** Bitdefender setzt bereits seit 2009 maschinelles Lernen ein und sorgt so für eine optimierte Bedrohungserkennung mit geringer Fehlalarmquote, die auch unbekannte Bedrohungen vor bzw. während der Ausführung abwehrt
- **Hyperdetect - individuell anpassbares maschinelles Lernen- Ermöglicht es IT-Teams, den Schutz auf besonders sensible Hochrisiko- Unternehmensdienste abzustimmen**
- **Anomalieerkennung:** Mittels fortschrittlicher maschineller Lernverfahren werden Systemdienste analysiert und Abweichungen von der Norm sofort erkannt, um auch gut getarnte Angriffe aufzudecken. So können auch unternehmensspezifische Anwendungen vor Angriffen geschützt werden
- **Cloudbasierte Sandbox:** Erkennt komplexe Bedrohungen schon vor der Ausführung, indem verdächtige Dateien zur weiteren Analyse automatisch an eine Cloud-Sandbox übermittelt und abhängig von der jeweiligen Bewertung geeignete Bereinigungsmaßnahmen eingeleitet werden
- **Network Attack Defense:** Erkennt und blockiert auch neue Bedrohungsarten schon in frühen Phasen der Angriffskette, so z B Brute-Force-Angriffe, Passwortdiebstahl und laterale Bewegungen
- **Exploit-Abwehr:** Gleich mehrere Exploit Prevention Engines schützen den Arbeitsspeicher und blockieren Angriffe, bevor sie Schwachstellen im System ausnutzen, und senken so Priorisierungsaufwand
- **Abwehr von dateilosen Angriffen:** Erkennt und blockiert skriptbasierte, dateilose, schwer aufzuspürende und speziell angepasste Malware mit automatischer Bereinigung
- Integrierte Client-Firewall, Gerätesteuerung, Filter für Webinhalte, Anwendungssteuerung und vieles mehr
- **Ransomware-Abhilfe:** Erstellt in Echtzeit Sicherungskopien von Dateien, bevor sie durch

einen verdächtigen Prozess verändert werden, um das Risiko eines Datenverlusts bei komplexen Ransomware-Angriffen zu senken.

- **Add-on-Module:** E-Mail-Sicherheit, Full Disk Encryption, Patch Management

EDR mit wenig Aufwand

Funktionsreiche Tools für die Bedrohungsuntersuchung, die für Unternehmen jeder Größe entwickelt wurden

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.

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

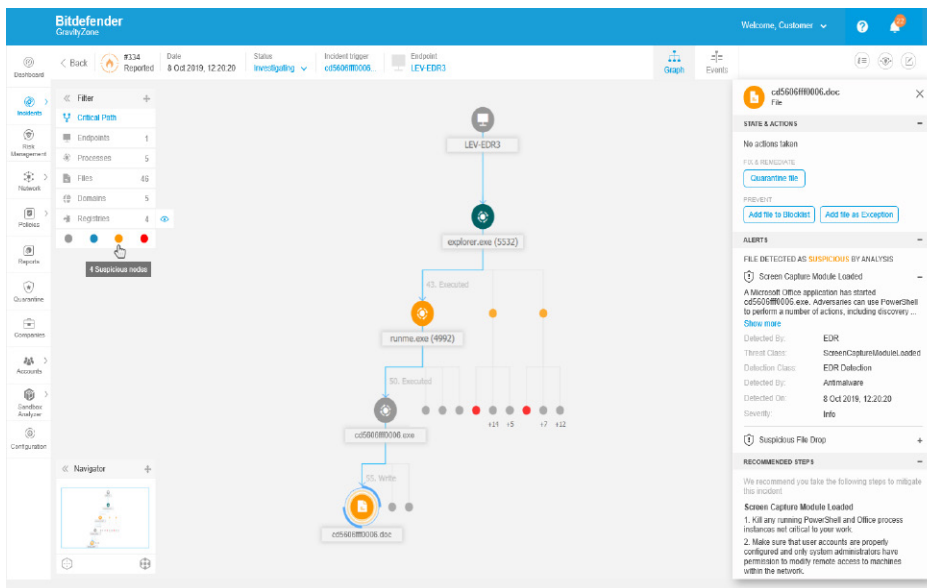
Intelligente Reaktionen für noch zuverlässigere Prävention

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.

Überwinden Sie den Mangel an Sicherheitsfachkräften und vermeiden Sie Überlastung durch übermäßige Alarmmeldungen

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-Präventionstechnologien und die

verhaltensbasierte Prozessprüfung bei Ausführung neutralisiert. Automatische Reaktionen und Reparaturen machen menschliches Eingreifen bei blockierten Angriffen unnötig.

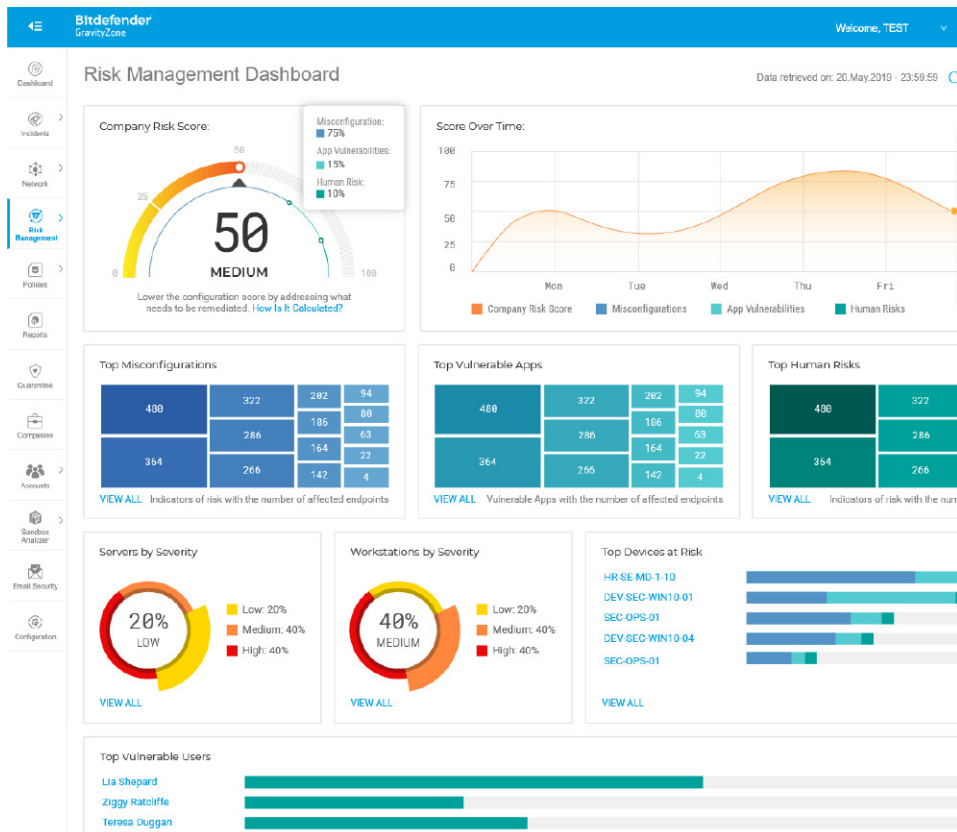


Die erweiterte Erkennung und Reaktion zeigt genau, wie sich eine potenzielle Bedrohung auf Ihre Umgebung auswirkt. MITRE-Angriffstechniken und Indicators of Compromise (IoC) bieten einen stets aktuellen Einblick in die genannten Bedrohungen und andere möglicherweise beteiligte Malware. Eine übersichtliche visuelle Darstellung zeigt kritische Angriffspfade und entlasten das IT-Personal.

Risikoanalysen für Endpunkte und Benutzerverhalten zur kontinuierlichen Reduzierung der Angriffsfläche

Ermöglicht aktive Systemhärtungsprozesse im gesamten Unternehmen

Bitdefenders Engine für die Endpunkt-Risikoanalyse ermöglicht es Unternehmen, Fehlkonfigurationen und Einstellungen im Zusammenhang mit der Endgerätesicherheit kontinuierlich zu bewerten, zu priorisieren und zu beheben. Grundlage dafür ist eine benutzerfreundliche und nach Prioritäten geordnete Liste. Mit seiner einzigartigen Risikoanalyse von Endpunkten und Benutzerverhalten ermöglicht GravityZone eine kontinuierliche Reduzierung der Angriffsfläche.



GravityZone Ultra Risikomanagement-Dashboard. Erhalten Sie eine allgemeine Risikobewertung für Ihr Unternehmen und erfahren Sie, inwieweit einzelne Fehlkonfigurationen, Anwendungsschwachstellen und Benutzerverhalten dazu beitragen.

Integration mit Drittanbieterlösungen

Unterstützt die Integration mit Ihren bestehenden Sicherheitstools (einschließlich Splunk) und wurde für Rechenzentrumstechnologien einschließlich aller gängigen Hypervisoren optimiert.

Weitere Informationen und detaillierte Systemanforderungen finden Sie unter <https://www.bitdefender.com/business/enterprise-products/ultra-security.html>

Oder wenden Sie sich direkt an Ihren Bitdefender-Partner vor Ort.

Bitdefender®

Gründung 2001 in Rumänien
Anzahl der Mitarbeiter 1800+

Hauptsitz
Unternehmenszentrale – Santa Clara, Kalifornien, USA
Technologiezentrum – Bukarest, Rumänien

NIEDERLASSUNGEN AUF DER GANZEN WELT
USA & Kanada: Ft. Lauderdale, Florida | Santa Clara, Kalifornien | San Antonio, Texas | Toronto, Kanada
Europa: Kopenhagen, DÄNEMARK | Paris, FRANKREICH | München, DEUTSCHLAND | Mailand, ITALIEN | Bukarest, Iasi, Cluj, Timisoara, RUMÄNIEN | Barcelona, SPANIEN | Dubai, VAE | London, GB | Den Haag, NIEDERLANDE
Australien: Sydney, Melbourne