Datenblatt

GravityZone Security
EDR Cloud

Fortschrittliche Endpoint Detection and Response

Cyber-Kriminelle werden immer raffinierter, ihre modernen Angriffstechniken immer schwerer abzufangen. Mit Techniken, die für sich genommen wie gewöhnliche Prozesse aussehen, sind die heutigen Täter in der Lage, sich Zugang zu Infrastrukturen zu verschaffen und dort monatelang unbemerkt zu bleiben, was das Risiko kostspieliger Datenpannen deutlich erhöht. Wenn Ihre vorhandene Endpoint-Sicherheitslösung komplexe Angriffe nicht zuverlässig erkennen und abwehren kann, können Sie mit GravityZone EDR Cloud Ihren Sicherheitsbetrieb schnell und effektiv stärken.

GravityZone EDR Cloud überwacht Ihr Netzwerk, um verdächtige Aktivitäten frühzeitig zu erkennen, und liefert wirksame Tools zur Abwehr von Cyberangriffen. Es vereint Bitdefender preisgekrönte maschinelle Lernverfahren, Cloud-Scans und Sandbox-Analysen, um auch solche Aktivitäten aufzuspüren, die herkömmliche Schutzmechanismen am Endpoint umgehen. Es liefert lückenlose Einblick in die Techniken, Taktiken und Prozeduren (TTPs), die bei aktiven Angriffen zum Einsatz kommen, und bietet gleichzeitig umfassende Suchmöglichkeiten nach bestimmten Gefährdungsanzeichen (IoCs), MITRE ATT&CK-Techniken und anderen Artefakten, um Angriffe frühzeitig zu erkennen.

Bitdefender EDR Cloud liefert innovative und aussagekräftige visuelle Darstellungen, die mit Kontext und Bedrohungsinformationen angereichert werden, und dem IT-Team Angriffspfade und Sicherheitslücken aufzeigen. So können Vorfalluntersuchung und -reaktion deutlich abgekürzt und die IT-Abteilung nachhaltig entlastet werden. Mit dem Sandbox Analyzer können verdächtige Dateien in einer kontrollierten virtuellen Umgebung ausgeführt und so bei Bedarf isoliert und neutralisiert werden. Die GravityZone EDR Cloud-Funktionen schützen Unternehmen vor modernen Bedrohungen und ermöglichen gleichzeitig eine proaktive Bedrohungssuche und Ursachenanalyse.

Was leistet GravityZone EDR Cloud?

- **Erkennt komplexe Angriffe und wehrt sie ab.** Überwacht Ihr Netzwerk, um verdächtige Aktivitäten frühzeitig zu erkennen, und liefert wirksame Tools zur Abwehr von Cyberangriffen.
- **Kommt ohne Sicherheitsfachkräfte aus.** Ermöglicht Teams ein schnelles Eingreifen durch automatisch priorisierte Warnmeldungen und Vorfallreaktionen mit nur einem Klick.
- **Reduziert Risiken für das Unternehmen.** Führt anhand hunderter Faktoren kontinuierliche Risikoanalysen für Ihre Infrastruktur durch und mindert so die Risiken die von Benutzern, Netzwerk und Betriebssystemen ausgehen.

Bitdefender
BUILT FOR RESILIENCE

Zusammengefasst

Bitdefender EDR Cloud erkennt komplexe Bedrohungen wie dateilose Angriffe, Ransomware und andere Zero-Day-Bedrohungen in Echtzeit. Bedrohungsanalysen und cloudbasierte Ereignissammlung gewährleisten ein durchgehende Überwachung der Endpoints. Sicherheitsereignisse werden in einer Prioritätenliste zusammengefasst, die für weitere Untersuchungen und Reaktionen zur Verfügung steht. Bitdefender EDR liefert innovative und aussagekräftige visuelle Darstellungen, die mit Kontext und Bedrohungsanalysen angereichert werden, und dem IT-Team Angriffspfade und Sicherheitslücken aufzeigen. So können Vorfalluntersuchung und -reaktion deutlich abgekürzt und die IT-Abteilung nachhaltig entlastet werden.

Hauptvorteile

- Branchenführende Erkennung: Erweiterte Bedrohungserkennung und Nachvollziehbarkeit bringen die Stärken von XDR beim Schutz von Endpoints zur Geltung. Umfassende Suchmöglichkeiten nach bestimmten Gefährdungsanzeichen (IoCs), MITRE ATT&CK-Techniken und anderen Artefakten, um Angriffe frühzeitig zu erkennen.
- Gezielte Vorfalluntersuchung und -reaktion: Durch die Visualisierung von Vorfällen auf Unternehmensebene können Sie schnell und effizient reagieren, laterale Ausbreitungen eindämmen und laufenden Angriffen ein Ende bereiten.
- Maximale Effizienz: Unser Agent, der sich durch schnelle Bereitstellung und geringen Wartungsaufwand auszeichnet, garantiert maximale Effizienz und Sicherheit bei minimalem Aufwand. Wenn Sie uns die Verwaltung Ihrer Lösung überlassen möchten, ist jederzeit an Upgrade auf Bitdefender Managed Detection and Response (MDR) möglich.

"Dank der EDR-Funktionen von GravityZone erhalten wir detaillierte Berichte darüber, wie Prozesse im Laufe eine Vorfalls beeinträchtigt wurden. So sparen wir sehr viel Zeit bei der Untersuchung von Vorfällen, da die manuelle Arbeit wegfällt."

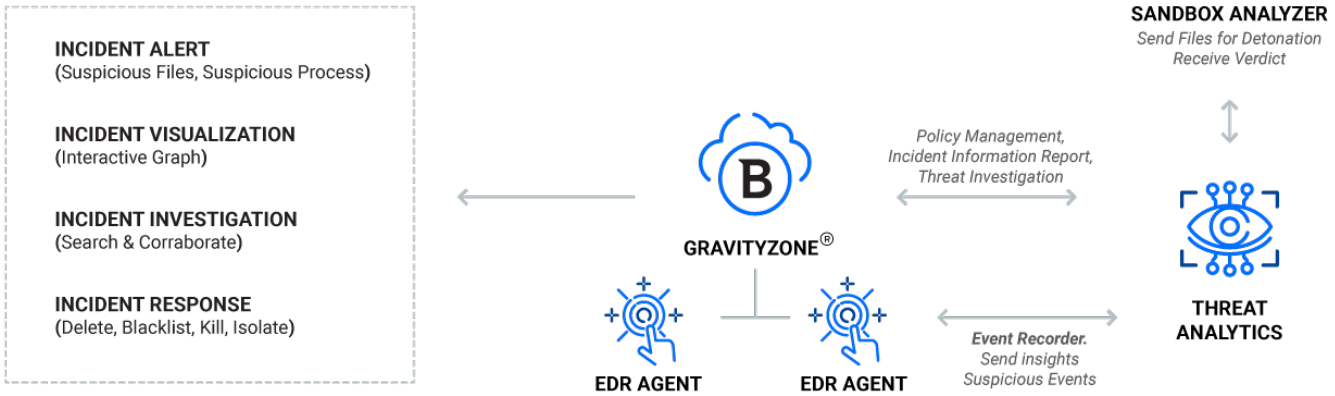
Sascha Neuhaus,
IT-Sicherheitsbeauftragter, Louis

- **Minimiert den Betriebsaufwand.** Die Agenten werden über die Cloud bereitgestellt und sind somit extrem wartungsarm. Sie lassen sich schnell und einfach bereitstellen. GravityZone EDR Cloud lässt sich zudem in Ihre bestehende Sicherheitsarchitektur integrieren, da die Lösung absolut kompatibel mit bestehenden Endpoint-Virenschutzlösungen ist.

Innovation für mehr Effizienz und Wirksamkeit

Bitdefenders Endpoint-übergreifende Korrelationstechnologie hebt die Bedrohungserkennung und -nachvollziehbarkeit auf ein neues Niveau, indem sie XDR-Funktionen zur Erkennung komplexer Angriffe in hybriden Infrastrukturen (Workstations, Server oder Container mit verschiedensten Betriebssystemen) Endpoint-übergreifend einsetzt. Sie erweitert die EDR-Nachvollziehbarkeits-, Analyse- und Ereigniskorrelationsfähigkeiten über die Grenzen einzelner Endpoints hinaus. So können Sicherheitsteams komplexen Cyberangriffen, an denen mehrere Endpoints beteiligt sind, noch wirksamer begegnen. Diese Endpoint-übergreifende Korrelationstechnologie verbindet die Detailtiefe und den umfangreichen Sicherheitskontext von EDR mit der infrastrukturübergreifenden Analysen von XDR (eXtended Detection and Response). Dank der visuellen Darstellungen von Bedrohungen auf Unternehmensebene können Unternehmen mit XDR gezielte Untersuchungen anstellen und effektiver reagieren.

Und so funktioniert es



Bitdefender EDR Cloud ist eine cloudbasierte Lösung auf Grundlage der Bitdefender GravityZone XDR-Plattform. Die EDR-Agenten werden auf den Endpoints Ihres Unternehmens installiert. Jeder EDR-Agent überwacht den Endpoint durchgehend, zeichnet relevante Daten und verdächtige Ereignisse auf und übermittelt sie gesichert an das zentrale GravityZone Control Center. Im Control Center führt die Endpoint-übergreifende Korrelationsengine von Bitdefender alle Ereignisse von den Endpoints komprimiert zusammen und generiert priorisierte Ansichten von Sicherheitsvorfällen auf Unternehmensebene, sodass Administratoren Bedrohungen zielgerichtet untersuchen und bekämpfen können.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender BSS GZ EDR Cloud Datasheet DEV4610 de DE
CD May 17 2022 VD May 17 2022