DATENBLATT

Ausschließlich für den Einsatz im Internet

Bitdefender

Endpoint Detection and Response

Komplexe Angriffe erkennen, gezielt untersuchen und effektiv abwehren

www.bitdefender.de

Die Cyber-Bedrohungslandschaft von Heute

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.

Wie schützt Bitdefender Endpoint Detection and Response (EDR)?

Wenn Ihre bestehende Endpunkt-Sicherheitslösung moderne, komplexe Angriffe nicht zuverlässig erkennen und abwehren kann, ist eine benutzerfreundliche Lösung wie Bitdefender Endpoint Detection and Response (EDR) eine willkommene Ergänzung für Ihre Sicherheitsstruktur.

Erkennung und Abwehr komplexer Angriffe

Bitdefender EDR prüft Ihr Netzwerk durchgehend auf verdächtige Aktivitäten, um Cyber-Angriffe frühzeitig zu erkennen, und enthält die nötigen Tools, um sie erfolgreich abzuwehren.

- EDR kombiniert Bitdefenders preisgekrönte maschinell lernende Algorithmen mit in die Cloud ausgelagerten Scans und dem Sandbox Analyzer und ist so in der Lage, Vorgänge aufzuspüren, die herkömmlichen Endpunktschutzmechanismen durch die Lappen gingen.
- Transparente Darstellung aller in Angriffen auf Ihr System verwendeten Techniken, Taktiken und Methoden
- Umfassende Suchmöglichkeiten nach bestimmten Gefährdungsanzeichen (IoC), MITRE ATT&CK-Techniken und anderen Artefakten, um Angriff frühzeitig zu erkennen. In der MITRE-ATT&CK-Auswertung von April 2020 schnitt Bitdefender bei der Erkennung und Warnung vor Gefahren in jeder Phase der gesamten Angriffskette hervorragend ab.
- Gezielte Reaktionen zur Schließung von Sicherheitslücken, um wiederholte Angriffe zu verhindern.

Qualifikationsdefizite in der Cyber-Sicherheit ausgleichen

- Intuitiv umsetzbare, vordefinierte Reaktionsabläufe machen es Sicherheitsteams leicht, schnell und effizient zu reagieren, laterale Ausbreitungen einzudämmen und laufende Angriffe abzubrechen.
- Visualisierungen der Bedrohungen helfen bei der gezielten Untersuchung, machen komplexe Funde verständlicher, ermitteln Angriffsursachen und helfen Ihnen, schnell und wirksam auf Vorfälle zu reagieren.
- Automatisierte Priorisierung von Warnmeldungen und Ein-Klick-Behebungsmöglichkeiten.

Risiken für das Unternehmen reduzieren

- Mit EDR wird Ihr Unternehmen mit speziell entwickelten Techniken durchgehend auf Hunderte von Faktoren überprüft, die auf ein Risiko hindeuten können. Die Lösung zeigt klare Wege und Möglichkeiten auf, um das Risiko für Benutzer, Netzwerk und Betriebssystem so gering wie möglich zu halten.

Betriebsaufwand minimieren

- EDR wird über die Cloud angeboten und ist somit extrem wartungsarm und lässt sich leicht in bestehende Sicherheitsarchitekturen integrieren, da es absolut kompatibel mit Ihrer Endpunkt-Virenschutzlösung ist.
- Der schlanke Agent benötigt nur wenig Speicherplatz, Arbeitsspeicher, Bandbreite und Rechenleistung.
- Die Lösung ist flexibel, skalierbar und jederzeit erweiterbar auf die vollständige Bitdefender-Endpunktsicherheitsplattform und auf Managed Detection and Response (MDR).

Und so funktioniert es

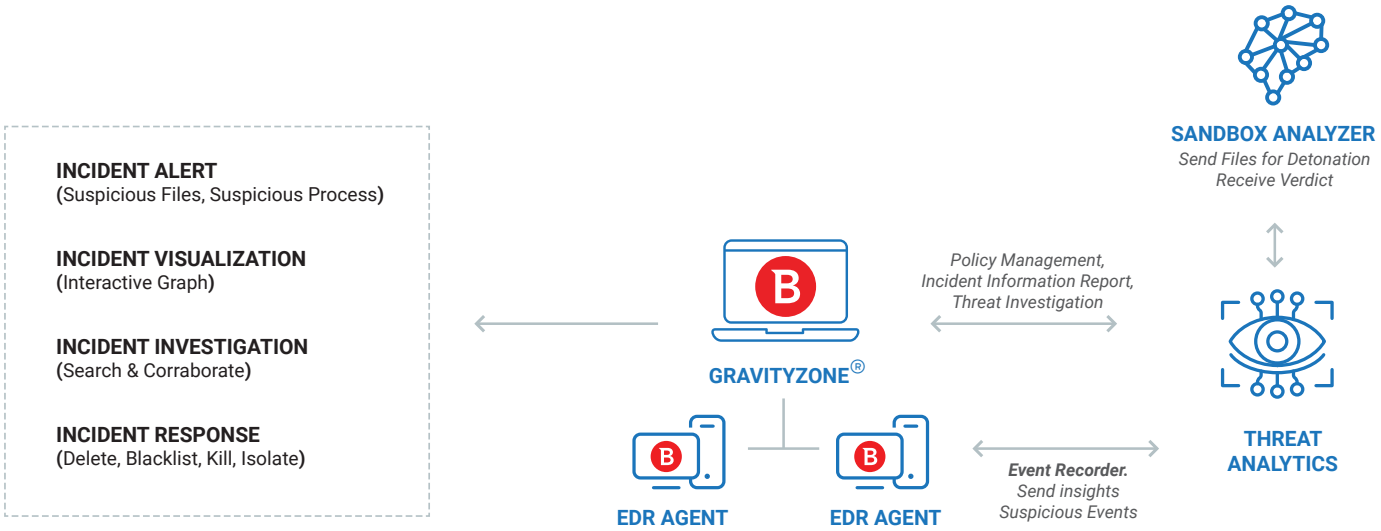

Abbildung: Bitdefender EDR

Bitdefender EDR ist eine Cloud-basierte Lösung auf der Grundlage der Bitdefender-GravityZone-Plattform. EDR-Agenten werden auf den Endpunkten des Unternehmens installiert. Jeder EDR-Agent überwacht den Endpunkt durchgehend, zeichnet relevante Ereignisse auf und überträgt sie gesichert an die GravityZone-Cloud.

In GravityZone werden die übermittelten Ereignisse gesammelt, analysiert und in einer Prioritätenliste zusammengefasst, die für weitere Untersuchungen und Reaktionen zur Verfügung steht. Verdächtige Dateien werden zur Detonation an den Sandbox Analyzer geschickt; die Bewertung aus der Sandbox-Detonation werden in den EDR-Vorfallsberichten vermerkt. Das EDR-Dashboard wird in Echtzeit aktualisiert und ist von beliebigen Geräten aus aufrufbar. So können Administratoren Benachrichtigungen und Visualisierung sehen, entsprechende Nachforschungen anstellen und effektiv auf Bedrohungen reagieren.

Komponenten und Funktionen von Bitdefender EDR

Risikoanalysen

Benutzer- und Endpunkt-bezogene Risikoanalysen
Auf der Grundlage von hunderten von Faktoren wird die Risikolage des Unternehmens kontinuierlich analysiert, um Risiken für Benutzer, das Netzwerk und die Endpunkte zu erkennen, zu priorisieren und zu beheben.

Erkennung

Branchenführende Erkennungstechnologie
Erkennt auch komplexe Bedrohungen wie dateilose Angriffe, Ransomware und andere Zero-Day-Bedrohungen in Echtzeit. Ergänzt Ihre bestehende Endpunktsicherheitslösung für noch mehr Sicherheit.

Bedrohungsanalysen
In der Cloud werden übermittelte Ereignisse gesammelt, analysiert und in einer Prioritätenliste zusammengefasst, die für weitere Untersuchungen und Reaktionen zur Verfügung steht.

Ereignisaufzeichnung
Ereignisse auf Endpunkten werden ununterbrochen beobachtet, um relevante Ereignisse an die Bedrohungsanalyseeinheit zu übermitteln und Visualisierungen von angriffsbezogenen Ereignissen zu erstellen.

Sandbox Analyzer
Führt verdächtige Dateien automatisch innerhalb einer kontrollierten virtuellen Umgebung aus. Das Ergebnis wird im Analysemodul ausgewertet, um Entscheidungen für den Umgang mit verdächtigen Dateien zu treffen.

Untersuchung und Reaktion

IoC-Prüfung
Abfragbare Ereignisdatenbank zur Aufdeckung von Bedrohungen. Aufspüren von MITRE-ATT&CK-Techniken und Gefährdungsanzeichen (IoC). Stets aktuelle Einblicke in bekannte Bedrohungen und andere möglicherweise beteiligte Malware.

Visualisierung
Angereichert mit Kontext und Bedrohungsanalysen zeigen klar verständliche visuelle Darstellungen kritische Angriffspfade auf – eine enorme Erleichterung für alle IT-Teams. Durch Ermittlung möglicher Sicherheitslücken und Angriffsauswirkungen kann die Compliance unterstützt werden.

Ausführung
Gezielte Sandbox-Untersuchungen helfen bei der Entscheidungsfindung im Umgang mit verdächtigen Dateien.

Blockierliste
Verbreitung verdächtiger Dateien oder Prozesse auf andere Maschinen unterbinden.

Prozessabbruch
Verdächtige Prozesse umgehend abbrechen, um potentielle Datenlecks zu verhindern.

Netzwerkisolation
Verbindungen von und zu Endpunkten blockieren, um laterale Bewegungen und weitere Datenpannen zu verhindern, während die Untersuchungen laufen.

Remote Shell
Aus der Ferne Befehle auf jeder beliebigen Maschine ausführen um unmittelbar auf aktuelle Vorfälle reagieren zu können.

Reporting- und Alarmfunktion

Dashboards und Berichte
Konfigurierbare Dashboards und umfassende Berichterstellung (geplante und Sofortberichte)

Benachrichtigungen
Konfigurierbares Dashboard und E-Mail-Benachrichtigungen

SIEM-Integration und API-Unterstützung
Weitere Integration mit Drittanbieter-Software möglich

Leistung und Verwaltung

Optimierter EDR-Agent
Geringe Anforderungen an Rechenleistung, RAM und Speicherplatz

Web-Konsole
Benutzerfreundliche Verwaltung in der Cloud

WARUM BITDEFENDER?

UNANGEFOCHTENER INNOVATIONSFÜHRER.

38 % der Cybersicherheitsanbieter weltweit haben mindestens eine Bitdefender-Technologie in ihre Produkte integriert. Wir sind in 150 Ländern vertreten.

WELTWEIT ERSTER ANBIETER VON LÜCKENLOSER SICHERHEIT

Die erste Sicherheitslösung, die Härtung, Prävention, Erkennung und Reaktion für Endpunkt, Netzwerk und Cloud vereint.

BESTBEWERTETE SICHERHEIT. VIELFACH BESTÄTIGT.

AV comparatives CERTIFIED ATP Enterprise 2019

AV comparatives Product of the Year 2019

FORRESTER WAVE LEADER 2019 Cloud Workload Security

BITDEFENDER GravityZone Ultra v6.6.7.166 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED

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

IM ZEICHEN DES WOLFS

Die Herausforderung des Fachgebietes Datensicherheit liegt darin, dass nur der klarste Blick, der schärfste Verstand und der tiefste Einblick gewinnen kann - Fehler sind keine Option. Unsere Aufgabe ist es, jedes Mal zu gewinnen, tausendmal aus 1.000 und 1 Million mal aus 1.000.000.

Und das tun wir. Wir sind der Leader in der Branche, jedem Hacker und Sicherheitsexperten um Schritte voraus. Der Scharfsinn unseres kollektiven Bewusstseins wird durch einen **hellleuchtenden Drachen-Wolf** repräsentiert. Er steht Ihnen zur Seite und schützt Sie mit seiner aus unserer Ingenieurskunst hervorgegangen Intuition vor allen Gefahren, die in den verborgenen Tiefen der digitalen Welt lauern.

Dieser Scharfsinn ist unsere Superkraft und bildet den Kern all unserer richtungsweisenden Produkte und Lösungen.

Bitdefender-EDR-DS-WebUseOnly-creat4933-de_DE
1/16/20November 16, 2020 9:20 pm1/16/20