GRAVITYZONE BUSINESS SECURITY

TAROX SECURITY
www.tarox.de/security

TAROX

GRAVITYZONE BUSINESS SECURITY

Bitdefender GravityZone ist eine ressourcenschonende Sicherheitslösung, durch Ihre optimale Leistung, umfassenden Schutz und durch ihre einfache Bereitstellung, Die zentrale Verwaltung, wird wahlweise in der Cloud oder mit der im eigenen Rechenzentrum gehostete Konsole, angewendet.

GravityZone Business Security wurde speziell für den Schutz kleiner bis mittelständischer Unternehmen entwickelt und kann dabei auf beliebig vielen Dateiservern, Desktops oder Laptops, physischen oder virtuellen Maschinen, eingesetzt werden. Business Security basiert auf einer mehrstufigen Endpunktsicherheitsplattform der nächsten Generation und bietet auf Grundlage von bewährten maschinellen Lernverfahren, Verhaltensanalysen und durchgehender Prozessüberwachung umfassende Funktionen zur Prävention, Erkennung und Blockierung von Bedrohungen, die am Markt ihresgleichen suchen.

Gewinner der jährlichen AV-Comparatives-Auszeichnung für herausragende Ergebnisse in allen Bereichen, einschließlich Schutzwirkung, Geschwindigkeit, Malware-Entfernung und geringe Fehlalarmquote.

HIGHLIGHTS

- Mehrstufige Sicherheitslösung der nächsten Generation, die konsequent erstklassige Prävention, Erkennung und Bereinigung aller Arten von Bedrohungen gewährleistet.
- Setzt auf maschinelles Lernen, fortschrittliche Heuristiken, erweiterte Funktionen für den Exploit-Schutz und weitere proprietäre Verfahren zum Schutz von Endpunkten.
- Beste Schutzwirkung und Leistung laut unabhängigen Vergleichstests
- Proaktive Härtung und Risikoanalyse zur kontinuierlichen Reduzierung der Angriffsfläche
- Netzwerkbasierte Sicherheit zum Schutz vor Angreifern, die sich über Schwachstellen im Netzwerk Zugriff zu Ihrem System verschaffen wollen

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

HAUPTFUNKTIONEN

Maschinell lernender Malware-Schutz

Verfahren für das maschinelle Lernen nutzen gut konfigurierte Maschinenmodelle und Lernalgorithmen, um komplexe Angriffe vorherzusagen und aufzuhalten. Die Bitdefender-Modelle für Machine Learning verwenden rund 40.000 statische und dynamische Eigenschaften und werden fortlaufend anhand von vielen Milliarden unbedenklichen und schädlichen Dateien weiter entwickelt, die von mehr als 500 Millionen Endpunkten weltweit bezogen wurden. So kann die Effektivität der Malware-Erkennung erheblich gesteigert und die Zahl der Fehlalarme minimiert werden.

Process Inspector

Der Process Inspector vertraut nichts und niemandem und überwacht durchgehend jeden einzelnen Prozess, der im Betriebssystem läuft. Die Software spürt verdächtige Aktivitäten oder ungewöhnliches Prozessverhalten auf, z. B. 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 und mehr. Der Process Inspector wendet angemessene Bereinigungsaktionen an, z.B. die Beendigung des Prozesses oder die Rückgängigmachung von Änderungen, die dieser Prozess vorgenommen hat. Er hat sich dabei als äußerst effektiv bei der Erkennung unbekannter komplexer Malware wie Ransomware erwiesen.

Leistungsstarker Schwachstellenschutz

Die Exploit-Abwehr-Technologie schützt den Speicher und besonders anfällige Anwendungen wie Browser, Dokumentanzeigeprogramme, Mediendateien und Laufzeit (z. B. Flash, Java). Komplexe Mechanismen überwachen Routinen für den Speicherzugriff, um Exploit-Verfahren wie API-Caller-Verification, Stack Pivot, Return-Oriented Programming (ROP) und weitere andere, um zu identifizieren und abzuwehren. Die GravityZone-Technologie kann fortschrittliche, schwer erkennbare Exploits bewältigen, mit denen gezielte Angriffe durchgeführt werden, um in eine Infrastruktur vorzudringen.

Steuerung und Absicherung von Endpunkten

Die richtlinienbasierte Endpunktsteuerung umfasst die Firewall, die Gerätesteuerung mit USB-Scans sowie die Inhaltssteuerung mit URL-Kategorisierung.

Phishing-Schutz und Web-Sicherheits-Filter

Mithilfe von Web-Sicherheitsfiltern kann der eingehende Internet-Datenverkehr (einschließlich SSL-, HTTP- und HTTPS-Datenverkehr) gescannt werden, um zu verhindern, dass die Malware auf Endpunkte heruntergeladen wird. Der Phishing-Schutz blockiert automatisch alle Phishing-Seiten und auch andere betrügerische Webseiten.

Network Attack Defense

Stärken Sie Ihren Schutz vor Angreifern, die versuchen, sich über Schwachstellen im Netzwerk Zugriff zu Ihrem System zu verschaffen. Erweitern Sie Ihre geschützten Bereiche mit netzwerkbasierter Sicherheit, die Bedrohungen wie Brute-Force-Angriffe, Passwortdiebstahl, Netzwerk-Exploits und laterale Bewegungen blockiert, bevor sie überhaupt ausgeführt werden können.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

GravityZone Email Security (Add-on)

Diese ultimative mehrstufige E-Mail-Sicherheitslösung schützt Ihr gesamtes Unternehmen vor bekannten, unbekannten und aufkommenden Bedrohungen der E-Mail-Sicherheit. Lässt groß angelegten Phishing-Angriffen, gezielten Angriffen, CEO-Betrug und Malware-Downloads keine Chance. Diese Funktion ist als Add-on zu GravityZone Business Security erhältlich.

Full Disk Encryption (Add-on)

Die vollständige Laufwerksverschlüsselung wird durch die GravityZone verwaltet, basierend auf Windows BitLocker und Mac FileVault. Die GravityZone nutzt die Vorteile, der in die Betriebssysteme eingebauten Technologien. Diese Funktion ist als Add-on zu GravityZone Business Security erhältlich.

Patch Management (Add-on)

Ungepatchte Systeme machen Unternehmen anfällig vor Malware-Vorfälle, Virenausbrüche und Datensicherheitsverletzungen. GravityZone Patch Management ermöglicht es Ihnen, Ihre Betriebssysteme und Anwendungen über die gesamte installierte Windows-Basis hinweg jederzeit auf dem neuesten Stand zu halten, egal ob Arbeitsplatzrechner, physische oder virtuelle Server. Diese Funktion ist als Add-on zu GravityZone Business Security erhältlich.

Reaktion und Isolierung

GravityZone bietet die besten Bereinigungsfunktionen auf dem Markt. Die Software blockiert und isoliert Bedrohungen automatisch, terminiert gefährliche Prozesse und macht Änderungen rückgängig.

Ransomware-Schutz

Die Lösung wurde anhand von Billionen Mustern, mit über 500 Millionen Endpunkten in aller Welt, trainiert. Egal, wie sehr Ransomware oder andere Malware auch modifiziert wird, Bitdefender erkennt neue Ransomware-Muster zuverlässig sowohl vor als auch während der Ausführung.

Die umfassendste intelligente Sicherheit in der Cloud

Mit über 500 Millionen geschützten Computern führt das Bitdefender Global Protective Network jeden Tag 11 Milliarden Anfragen durch und setzt dabei auf maschinelles Lernen und Ablauf Zusammenhänge, um Bedrohungen zu erkennen, ohne den Benutzer zu beeinträchtigen.

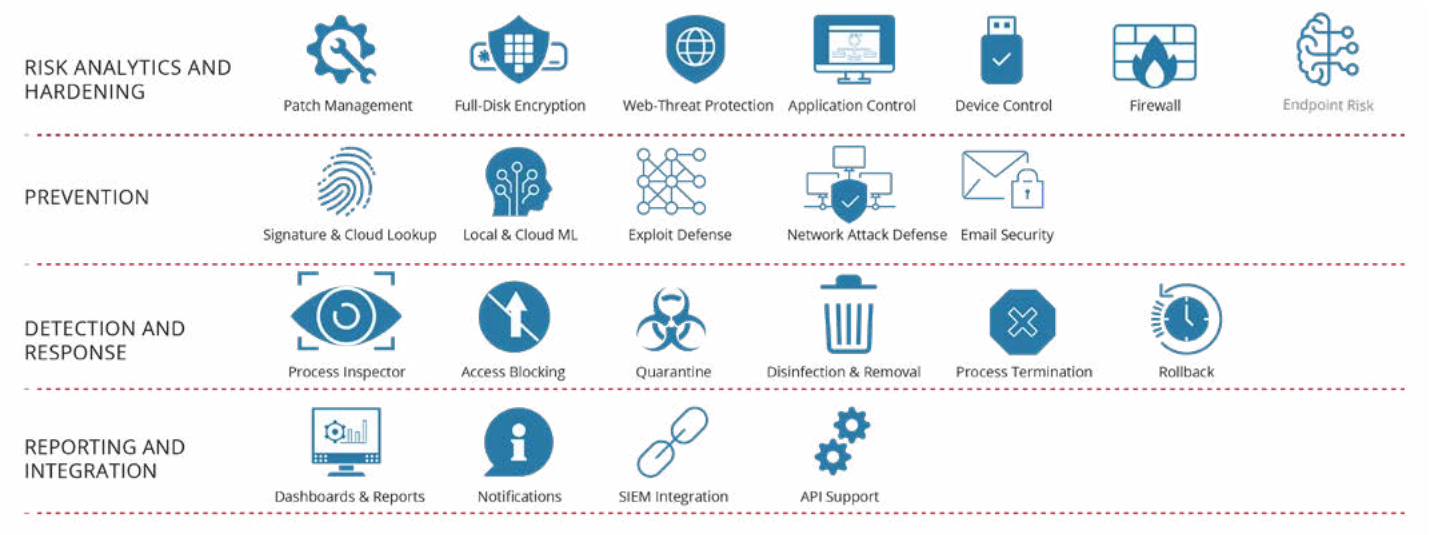
Automatisierte Reaktion und Bereinigung von Bedrohungen

Sobald eine Bedrohung gefunden wurde, wird diese sofort von der GravityZone BS neutralisiert, u.a. durch den Abbruch von Prozessen, das Verschieben in die Quarantäne und das Entfernen und Rückgängig machen von schädlichen Änderungen. Die Lösung tauscht in Echtzeit Daten mit dem GPN (Global Protective Network) aus, dem Bitdefenders Cloud-basiertem Gefahrenanalysedienst. Auf diesem Weg können ähnliche Angriffe überall auf der Welt verhindert werden.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

Endpunkt-Risikoanalyse

Die Risikoanalyse-Engine errechnet kontinuierlich eine Risikobewertung, um die Sortierung und Priorisierung von Assets zu erleichtern und Administratoren eine schnelle Reaktion auf die dringlichsten Probleme zu ermöglichen. Rückgängig machen von schädlichen Änderungen. Die Lösung tauscht in Echtzeit Daten mit dem GPN (Global Protective Network) aus, dem Bitdefenders Cloud-basiertem Gefahrenanalysedienst. Auf diesem Weg können ähnliche Angriffe überall auf der Welt verhindert werden.



GravityZone Business Security basiert auf einer mehrstufigen Endpunktsicherheitsplattform der nächsten Generation und bietet auf Grundlage von bewährten maschinellen Lernverfahren, Verhaltensanalysen und durchgehender Prozessüberwachung umfassende Funktionen zur Prävention, Erkennung und Blockierung von Bedrohungen, die am Markt ihresgleichen suchen.

GravityZone Control Center

Das GravityZone Control Center ist eine integrierte und zentrale Verwaltungskonsole, über die alle Komponenten der Sicherheitsverwaltung auf einen Blick einsehbar sind. 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.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

VORTEILE

Mehr Effizienz im Betrieb durch nur einen einzigen Agenten und eine integrierte Konsole

Da Bitdefender nur einen einzigen integrierten Endpunktsicherheitsagenten einsetzt, kommt es nicht zur Agentenüberfrachtung. Der modulare Aufbau bietet höchste Flexibilität und lässt Administratoren Sicherheitsrichtlinien einrichten. GravityZone passt das Installationspaket automatisch und individuell an und minimiert so den Ressourcenverbrauch des Agenten. GravityZone ist von Grund auf als einheitliche, umfassende Sicherheitsverwaltungsplattform ausgelegt die physische, virtuelle und Cloud-Umgebungen gleichermaßen zuverlässig schützt.

- Setzen Sie auf eine leistungsstarke und einfache Lösung und machen Sie neue Server, Wartung und weitere IT-Mitarbeiter überflüssig
- Schnelle Inbetriebnahme dank integrierter Richtlinienvorlagen
- Zentrale Verwaltung über eine zentrale Oberfläche
- Reduzierte Kosten und zentrale Sicherheit für beliebig viele Benutzer
- Durch die zentrale Verwaltung müssen sich Mitarbeiter nie wieder um die Aktualisierung, Überwachung und Problembehandlung bei der Sicherheit kümmern und können sich voll und ganz auf ihre Arbeit konzentrieren.
- Einfache Bereitstellung per Fernzugriff
- Detaillierte Berichte - Erfahrene Administratoren können detaillierte Richtlinieneinstellungen vornehmen, die Lösung ist aber auch ohne IT-Kenntnisse leicht zu verwalten
- Updates erfolgen automatisch und Benutzer können die Einstellungen nicht verändern oder den Schutz deaktivieren. Somit ist das Unternehmen stets sicher,
- Wenden Sie Richtlinien anhand von Standort oder Benutzer an und seien Sie flexibel bei der Vergabe von Freiheiten; sparen Sie bei der Anlage neuer Richtlinien Zeit; indem Sie bereits vorhandene wiederverwenden.

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

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

MANAGED DETECTION & RESPONSE (MDR)

TAROX SECURITY
www.tarox.de/security

TAROX

BITDEFENDER MDR: MACHEN SIE IHR UNTERNEHMEN CYBERRESILIENT

Cybersicherheit ist zu einem kritischen Faktor für den Geschäftserfolg geworden. Angreifer gehen immer raffinierter vor und herkömmliche Präventionsmethoden sind ihren Techniken kaum noch gewachsen. Für Unternehmen ist heute wichtiger denn je, dass Sie auf das notwendige Fachwissen für eine wirksame Bedrohungssuche zurückgreifen können. Nur so wird sichergestellt, dass sie umgehend reagieren und die Auswirkungen von Angriffen schnell und wirksam minimieren können.

Bitdefender MDR unterstützt Sie dabei, die Cyberresilienz Ihres Unternehmens zu stärken. Unsere Sicherheitsexperten sind rund um die Uhr für Sie im Einsatz und übernehmen mit fortschrittlichen Präventions-, Erkennungs- und Reaktionsverfahren die Verantwortung für Ihre Systeme.

Dabei profitieren Sie nicht nur von der branchenweit anerkannten Endpoint-Technologie GravityZone® Business Security Enterprise und ihrem breiten Funktionsumfang, sondern auch von dediziertem Support und einem geführten Onboarding-Prozess gepaart mit der Sicherheitsexpertise im Global Security Operations Center (SOC) von Bitdefender. So steht einem schnellen Start nichts mehr im Wege.

Bitdefender MDR umfasst zudem die regelmäßige proaktive Suche nach Bedrohungen, die sich gegen Ihre Unternehmenssysteme richten. Hinzu kommt ein risikogesteuertes Threat Hunting, das sich die Erkenntnisse von Expertenanalysen der globalen Bedrohungslandschaft zunutze macht. Egal, ob Mittelständler oder Großkonzern, Finanzdienstleister oder Online-Händler, Bitdefender MDR macht Unternehmen cyberresilient - wir lassen Angreifern keinen Platz zum Verstecken.

GRAVITYZONE XDR FOR MDR

Moderner Sicherheitsbetrieb erfordert eine Kombination aus Kontextinformationen, Fachwissen und Intuition, um auch schädliche Aktivitäten zu erkennen, die in der Lage sind, Sicherheitstools zu umgehen. Die präzise und korrelierte Erkennung und schnellen Reaktionsmaßnahmen mit GravityZone XDR for MDR ermöglichen es unserem Sicherheitsteam, Angriffen über Ihre gesamte Infrastruktur hinweg auf die Spur zu kommen und sie zu analysieren. Unsere Cyberebdrohungsjägern erhalten deutlich mehr Kontextinformationen, indem es sie in allen Details nachvollziehen lässt, wie sich die von uns geschützten Umgebungen unter “normalen” Umständen verhalten. GravityZone XDR for MDR ist ab sofort verfügbar und lässt Sie Ihren MDR-Dienst um frei wählbare Sensoren erweitern:

- Produktivitätsanwendungen
- Cloud
- Identität
- Netzwerk

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

ZUSAMMENGEFASST

Mit Bitdefender MDR meistern Sie die Sicherheitsherausforderungen von heute, damit Sie Ihnen morgen kein Kopfzerbrechen mehr bereiten. Ihre IT ist mit der schieren Anzahl an Warnmeldungen überfordert, Tools sind zu komplex, es fehlt an Ressourcen und Fachkräften oder Sie befürchten Compliance- und Datenschutzprobleme? Bitdefender MDR schafft Cyberresilienz und schützt Ihre Mitarbeiter, Systeme und Daten rund um die Uhr.

Wir bieten Ihnen neben dem Projektmanagement alle Dienstleistungen, die für eine reibungslose Einrichtung erforderlich sind, sodass Sie schnellstmöglich geschützt sind. Mit Ihrem Security Account Manager erhalten Sie zudem einen persönlichen Ansprechpartner, der Ihnen bei allen Belangen rund um Bitdefender MDR zur Seite steht.

Ihre MDR-Leistungen werden im Bitdefender MDR Portal zusammengefasst: Hier finden Sie individuelle Dashboards für Ihre Umgebungen, sämtliche Onboarding-Dokumente und Berichte und eine Übersicht aller laufenden Untersuchungen.

BITDEFENDER MDR SNAPSHOT

- Mehr als 85 hochqualifizierte Sicherheitsanalysten, Forscher und Bedrohungsjäger für Sie im Einsatz.
- Ja, es ist 3 Uhr morgens - aber wir kennen keine Pausen. Wir arbeiten rund um die Uhr, damit Sie es nicht müssen.
- Alle Bitdefender-Analysten sind mindestens einmal unabhängig zertifiziert.

„Bitdefender MDR gibt mir die Sicherheit, dass unser gesamtes Netzwerk in Echtzeit überwacht wird, auch wenn weder ich noch sonst irgendein Mitarbeiter im Büro ist. So können wir unsere Daten jederzeit schützen, egal von wo sich unsere Mitarbeiter einloggen. MDR ist gewissermaßen eine Erweiterung meines Teams, die mir hilft die Mission der Erzdiözese zu sichern.“

IT-Leiter
Erzdiözese | Gemeinnützige Organisation | USA

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

LASSEN SIE CYBERANGRIFFEN KEINE CHANCE MIT BITDEFENDER MDR

Bitdefender MDR ist in drei Service-Stufen verfügbar.

	Foundations	Premium	Enterprise
Rund um die Uhr im Einsatz	✓	✓	✓
Bedrohungsmanagement	✓	✓	✓
Vorfallreaktion anhand kundenspezifischer Strategien	✓	✓	✓
Expertenempfehlungen			
MDR-Portal	✓	✓	✓
Analyse von Ursachen und Auswirkungen	✓	✓	✓
Monatliche Berichte	✓	✓	✓
Risikogesteuerte Bedrohungssuche	✓	✓	✓
Benutzerdefinierte Benachrichtigung	✓	✓	✓
Optionale XDR-Add-ons	✓	✓	✓
Fester Ansprechpartner für Ihre Sicherheit		✓	✓
Gezielte Bedrohungssuche		✓	✓
Kundenspezifische Bedrohungsmodellierung		✓	✓
Überwachung beliebter Ziele			✓
Schutz von Marken und geistigem Eigentum			✓
Dark Web-Überwachung			✓

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

Im Bitdefender-MDR-Portal können Sie Ihre MDR-Leistungen jederzeit einsehen. Hier erhalten Sie zudem Zugriff auf individuelle Dashboards für Ihre Umgebungen, finden alle Onboarding-Dokumente und Berichte und können sich einen Überblick über laufende Untersuchungen verschaffen.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

KOMPLEXE ANGRIFFE ERKENNEN, GEZIELT UNTERSUCHEN UND EFFEKTIV ABWEHREN

Endpoint Detection and Response

TAROX SECURITY
www.tarox.de/security

TAROX

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.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

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

INCIDENT ALERT
(Suspicious Files, Suspicious Process)

INCIDENT VISUALIZATION
(Interactive Graph)

INCIDENT INVESTIGATION
(Search & Corraborate)

INCIDENT RESPONSE
(Delete, Blacklist, Kill, Isolate)

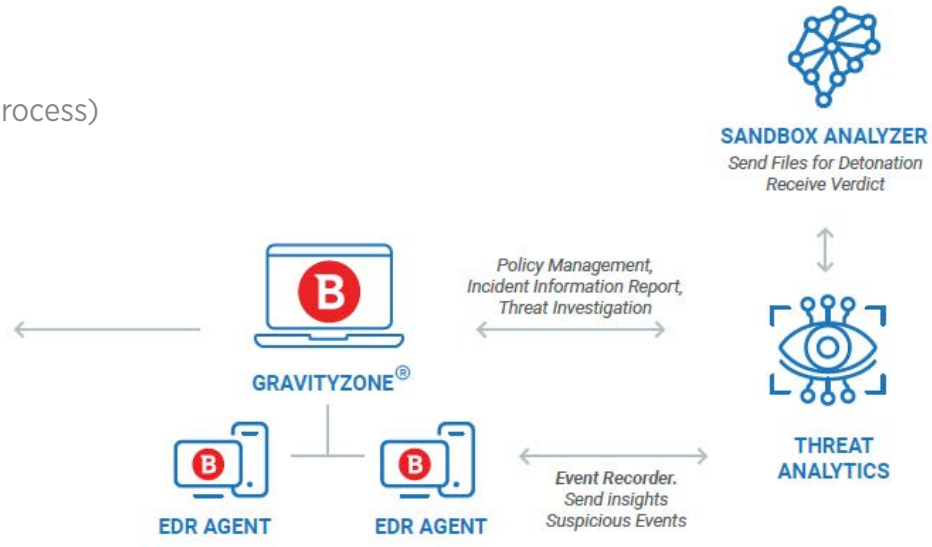


ABBILDUNG: BITDEFENDER EDR

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 EDRVorfallsberichten 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.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

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.

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

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

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de

TAROX Aktiengesellschaft Stellenbachstraße 49-51 | 44536 Lünen
T: +49 (0) 231/98 98 0-665 | E-Mail: security@tarox.de
Web: www.tarox.de