DATENBLATT

WATCHGUARD EPDR

Endpoint Protection, Detection and Response.

CYBERSICHERHEIT FÜR UNTERNEHMEN

Mobilität, Verarbeitung und Remote-Arbeit haben die Geschäftsumgebung revolutioniert. Endpoints sind das primäre Ziel der meisten Cyberangriffe. Daher müssen Sicherheitslösungen für Endpoints fortgeschritten, anpassungsfähig und automatisiert sein und bestmögliche Prävention und Erkennung bieten.

Unternehmen erhalten pro Woche Tausende von Warnmeldungen zu Malware, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % überhaupt geprüft werden. Ein Administrator für Cybersicherheit verbringt im Durchschnitt zwei Drittel der Zeit mit der Verwaltung von Malware-Warnmeldungen.

AUSGEREIFTE CYBERANGRIFFE

Abwehr neuartiger Bedrohungen

Mit modernen Mitteln geplante und ausgeführte Cyberangriffe sind darauf ausgelegt, dass sie den von traditionellen Sicherheitslösungen geleisteten Schutz umgehen. Diese Angriffe werden aufgrund der zunehmenden Professionalisierung der Hacker immer häufiger und ausgefeilter. Dies liegt auch daran, dass der Beseitigung von Sicherheitslücken in Systemen zu wenig Aufmerksamkeit geschenkt wird.

Somit wird klar, dass herkömmliche Schutzplattformen (EPPs) unzureichend sind. Sie liefern nicht ausreichend detaillierte Einblicke in die Prozesse und Anwendungen der Unternehmensnetzwerke. Hinzu kommt, dass einige EDR-Lösungen ineffizient sind, unnötigen Stress verursachen und die Arbeitsbelastung von Sicherheitsadministratoren erhöhen, da die Verantwortung für die Verwaltung von Warnmeldungen auf sie delegiert wird und sie Bedrohungen manuell klassifizieren müssen.

WATCHGUARD EPDR

Proaktive Erkennung von Bedrohungen und Threat Hunting

WatchGuard EPDR ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Die Plattform automatisiert die Prävention, Erkennung, Eindämmung und Abwehr mannigfaltiger, neuartiger Bedrohungen – von Zero-Day-Malware über Ransomware, Phishing oder In-Memory-Exploits bis hin zu weiteren Angriffsversuchen ohne Malware – für optimalen Schutz, heute und morgen, innerhalb und außerhalb des Unternehmensnetzwerks.

Im Gegensatz zu anderen Lösungen kombiniert sie eine sehr breite Palette an Schutztechnologien (EPP) mit automatisierten Funktionen für Erkennung und Reaktion. Die Lösung umfasst auch zwei Services, die von den Experten von WatchGuard verwaltet werden und in die Lösung integriert sind:

- Zero-Trust Application Service: 100%ige Klassifizierung von Anwendungen
- Threat Hunting Service: Erkennung von Hackern und Insidern

Dank seiner cloudbasierten Architektur ist der Agent ressourcensparend und hat nur minimale Auswirkungen auf die Leistungsfähigkeit der Endpoints, die über WatchGuard Cloud verwaltet werden. Mit WatchGuard Cloud können Sie das gesamte Portfolio über eine einzige, zentrale Ansicht verwalten, wodurch Infrastrukturkosten sinken und der Zeitaufwand für Reporting und betriebliche Aufgaben sinkt.

VORTEILE

Weniger Aufwand, geringere Sicherheitskosten

- Durch die verwalteten Services lassen sich Kosten für Fachpersonal einsparen. Außerdem müssen keine Fehlalarme untersucht werden und es werden keine Entscheidungen delegiert.
- Die verwalteten Services lernen automatisch von Bedrohungen. Es wird keine Zeit auf manuelle Einstellungen verschwendet.
- Keine Installation, Konfiguration oder Pflege einer Managementinfrastruktur erforderlich.
- Dank ressourcensparendem Agent und Cloudarchitektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Verkürzung der Erkennungszeit dank Automatisierung

- Blockiert Anwendungen, die ein Sicherheitsrisiko darstellen (durch Hash oder Prozessnamen).
- Verhindert die Ausführung von Angriffen, Zero-Day-Malware, Angriffen ohne Datei/Malware, Ransomware und Phishing-Versuchen.
- Erkennt und blockiert bösartige Aktivitäten im Arbeitsspeicher (Exploits), bevor diese Schaden anrichten können.
- Erkennt und unterbindet Techniken, Taktiken und Prozesse von Hackern.

Automatisierung und Verkürzung von Problemlösung und Reaktion

- Problemlösung und Reaktion: forensische Informationen zur gründlichen Untersuchung jedes Angriffsversuchs sowie Tools zur Verringerung der Auswirkungen (Desinfektion).
- Nachverfolgbarkeit jeder Aktion; verwertbare Erkenntnisse über den Angreifer und dessen Aktivitäten, was die forensische Untersuchung erleichtert
- Verbesserung und Anpassung von Sicherheitsrichtlinien aufgrund der Erkenntnisse aus der forensischen Analyse.

ERWEITERTE UND AUTOMATISIERTE ENDPOINT-SICHERHEIT

Traditionelle, auf Vorbeugung ausgerichtete Schutztechnologien (EPPs) sind kostengünstige Maßnahmen gegen bekannte Bedrohungen und böswillige Verhaltensweisen, reichen jedoch alleine nicht aus. Um ein Unternehmen erfolgreich zu schützen und Cyberbedrohungen ein Ende zu setzen, ist eine Abkehr von der traditionellen Prävention hin zu kontinuierlicher Prävention, Erkennung und Reaktion nötig. Dabei wird stets davon ausgegangen, dass dem Unternehmen Schaden zugefügt wurde und alle Endpoints ständig angegriffen werden.

WatchGuard EPDR vereint herkömmliche Präventionstechnologien mit innovativen, adaptiven Methoden der Prävention, Erkennung und Reaktion in einer einzigen Lösung, um moderne Cyberbedrohungen gegenwärtig und zukünftig abzuwehren:

Traditionelle Präventionsmethoden

- Persönliche oder verwaltete Firewall (IDS)
- Gerätesteuerung
- Ständige Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Verwaltete Deny List/Allow List
- Schwarmintelligenz
- Vorab-Ausführungs-Heuristik
- URL Filtering – Webbrowsing
- Phishingschutz
- Manipulationsabwehr
- Wiederherstellung und Zurücksetzung

Neuartige Sicherheitstechnologien

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Verhindert die Ausführung unbekannter Prozesse
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher Prozesse (APT, Ransomware, Rootkits usw.)
- Sandboxing in realen Umgebungen
- Verhaltensanalysen und Indicator-of-Attack(IoA)-Erkennung (Skripte, Makros usw.)
- Threat Hunting
- Computerisolierung
- Programmsperre nach Hash oder Name
- Grafische Darstellung der Angriffe

ZERO-TRUST-MODELL

Der Zero-Trust Application Service klassifiziert 100 % der Prozesse, überwacht die Aktivitäten an den Endpoints und unterbindet die Ausführung von Anwendungen und böswilligen Prozessen. Bei jeder Ausführung wird eine Echtzeit-Klassifizierung als böswillig oder rechtmäßig, ohne Unsicherheiten und ohne Delegierung von Entscheidungen an den Kunden versendet, wobei manuelle Prozesse vermieden werden. Möglich ist dies dank der Leistung, Geschwindigkeit, Anpassungsfähigkeit und Skalierbarkeit der KI und der Cloud-Verarbeitung.

Der Service vereint Big-Data-Technologien und mehrstufiges maschinelles Lernen einschließlich Deep Learning – das Ergebnis der laufenden Überwachung und Automatisierung der Erfahrungen und Kenntnisse, die das Bedrohungsteam von WatchGuard erworben hat.

Der verwaltete Service für Threat Hunting wird von einem Expertenteam ausgeführt, das anhand von Tools zur Profilerstellung und Ereigniskorrelation neue Hacking- und Ausweichtechniken proaktiv erkennt. Die Threat Hunter bei WatchGuard gehen bei ihrer Arbeit davon aus, dass Unternehmen ständig angegriffen werden.

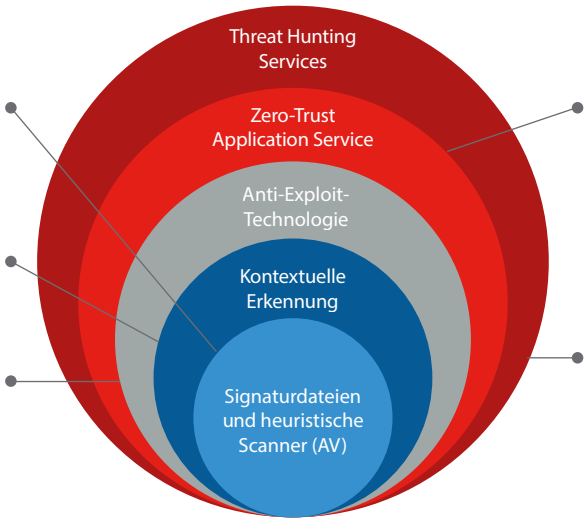
Zero-Trust Modell: Mehrschichtiger Schutz

ENDPOINT-EBENEN:

Ebene 1/Signaturdateien und heuristische Technologien
Effektive, optimierte Technologie zur Erkennung bekannter Angriffe

Ebene 2/Kontextuelle Erkennung
Erkennung von Angriffen ohne Malware und Dateien

Ebene 3/Anti-Exploit-Technologie
Erkennung dateiloser Angriffe, die Schwachstellen ausnutzen



CLOUDNATIVE EBENEN

Ebene 4/Zero-Trust Application Service
Erkennt, ob auf einer vorherigen Ebene ein Verstoß vorliegt, stoppt Angriffe auf bereits infizierten Computern und verhindert laterale Bewegungsangriffe innerhalb des Netzwerks

Ebene 5/Threat Hunting Service
Erkennung angegriffener Endpoints, früher Phasen eines Angriffs und verdächtiger Aktivitäten

Unterstützte Plattformen und Systemanforderungen von WatchGuard EPDR

Unterstützte Betriebssysteme: Windows (Intel & ARM), macOS (Intel & ARM), Linux und Android.
EDR-Funktionen sind unter Windows, macOS und Linux verfügbar, wobei Windows sämtliche Funktionen uneingeschränkt unterstützt.

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge und Opera.

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.