DATENBLATT

WATCHGUARD EPDR

Endpoint Protection Detection and Response

HERAUSFORDERUNGEN BEI DER CYBERSICHERHEIT FÜR UNTERNEHMEN

Endpoints sind das primäre Ziel der meisten Cyberangriffe. Da die Technologie-Infrastruktur zunehmend komplexer wird, haben Unternehmen Probleme, was Know-how und Ressourcen zur Überwachung von Endpoint-Sicherheitsrisiken und zum Umgang mit diesen angeht. Welche Arten von Herausforderungen müssen Unternehmen bewältigen, wenn sie Endpoint-Sicherheitslösungen einsetzen?

- **Alert Fatigue:** 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 zwei Drittel der Zeit mit der Verwaltung von Malware-Warnmeldungen.
- **Komplexität:** Zu viele unverbundene Tools für Cybersicherheit lassen sich von Sicherheitsexperten evtl. nur schwer verwalten – aufgrund der Anzahl der erforderlichen Technologien, der fehlenden internen Fähigkeiten und des Zeitaufwands zur Identifizierung von Bedrohungen.
- **Schlechte Performance:** Häufig erfordern Lösungen für Endpoint-Sicherheit die Installation und Verwaltung mehrerer Agents auf jedem überwachten Computer, Server und Laptop. Dies verursacht schwerwiegende Fehler, eine schlechte Performance und einen hohen Ressourcenverbrauch.

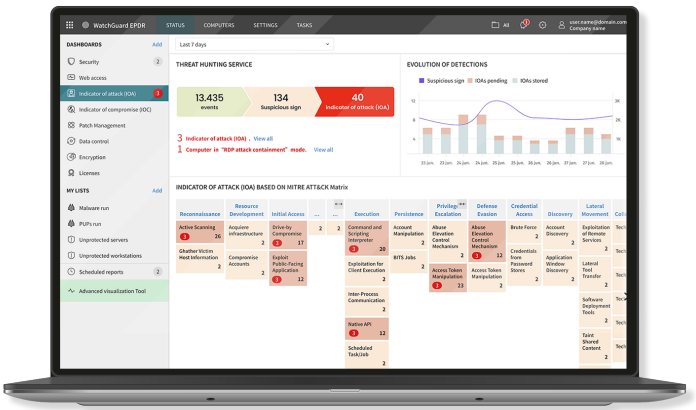
Traditionelle, auf Vorbeugung ausgerichtete Technologien für Endpoint-Schutz sind für bekannte Bedrohungen und böswillige Verhaltensweisen geeignet, bieten jedoch keinen ausreichenden Schutz vor modernen Cyberbedrohungen.

VON DER VORBEUGUNG BIS HIN ZUR REAKTION – AUTOMATISCHE ENDPOINT-SICHERHEIT

WatchGuard EPDR ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Die Plattform automatisiert die Vorbeugung, Erkennung, Eindämmung und Abwehr im Zusammenhang mit mannigfaltigen, neuartigen Bedrohungen – von Zero-Day-Malware über Ransomware, Phishing oder In-Memory-Exploits bis hin zu weiteren Angriffsversuchen ohne Dateien und Malware.

Im Gegensatz zu anderen Lösungen kombiniert sie eine sehr breite Palette an Technologien zum Endpoint-Schutz (EPP) mit automatisierten Funktionen für Erkennung und Reaktion (EDR). 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



WatchGuard EPDR vereint AV der nächsten Generation mit innovativem, adaptivem Schutz und EDR-Technologien in einer einzigen Lösung und ermöglicht es IT-Fachkräften, mit fortgeschrittenen Cyberbedrohungen fertigzuwerden:

AV-Technologien der nächsten Generation

- Persönliche oder verwaltete Firewall (IDS)
- Gerätesteuerung
- Kollektive Intelligenz und Heuristik vor der Ausführung
- Permanenter Multi-Vektor Anti-Malware & On-Demand-Scan
- URL Filtering, Webbrowsing und Anti-Phishing
- Manipulationsabwehr
- Automatische Behebung und Möglichkeit für Rollbacks
- Verschlüsselte Dateien über Schattenkopien wiederherstellen
- Schwachstellenanalyse

Neuartige Sicherheitstechnologien

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Cloudbasiertes maschinelles Erlernen von Verhaltensweisen ermöglicht die Klassifizierung sämtlicher Prozesse (APT, Ransomware, Rootkits usw.)
- Sandboxing in realen Umgebungen
- Schutz vor Exploits
- Netzwerkangriffsschutz: Verhindern, dass Angriffe Schwachstellen in über das Internet exponierten Diensten ausnutzen
- Threat Hunting: Verhaltensanalysen und Erkennung von IoA (Indicators of Attack) zur Identifizierung von LotL (Living off the Land-Angriffen)
- Indicators of Attack werden dem MITRE ATT&CK-Framework zugeordnet
- Erkennung und Abwehr von RDP-Angriffen
- Eindämmungs- und Bereinigungsmöglichkeiten wie Computerisolierung und Programmblockierung nach Hash oder Name

VORTEILE

Vereinfacht und maximiert Sicherheit

- Durch die automatischen Services lassen sich Kosten für Fachpersonal einsparen. Es müssen keine Fehlalarme untersucht werden, manuelle Einstellungen sind nicht erforderlich (weniger Zeitaufwand) und es werden keine Entscheidungen delegiert.
- Dank eines Agenten und der Cloudarchitektur wird die Leistungsfähigkeit der Endpoints nicht beeinträchtigt.

Benutzerfreundlich und einfach zu verwalten

- Mit dem Endpoint Security-Portfolio lassen sich alle Anforderungen des Endpoint-Schutzes auf bemerkenswert einfache Weise über eine einzige Webkonsole erfüllen.
- Einfach einzurichten. Zentrale plattformübergreifende Endpoint-Verwaltung.

Einzigartige EDR-Funktionen

- Zwölfmonatige Datenspeicherung und physisches Sandboxing in Echtzeit, um unbemerkte Hacker-Aktionen zu vermeiden.
- Zero-Trust Application Service: Klassifizierung jedes Prozesses basierend auf dem dynamischen Verhalten des Prozesses. Threat Hunting Service – zur Erkennung von Hackern und Insidern.

ZERO-TRUST-MODELL: MEHRSCHICHTIGER SCHUTZ

Die Endpoint Security-Plattform von WatchGuard nutzt nicht nur eine einzige Technologie, sondern verschiedene, um die Erfolgschancen eines Angreifers zu reduzieren. Gemeinsam verwenden diese Technologien Ressourcen am Endpoint, um das Risiko einer Sicherheitsverletzung zu minimieren.

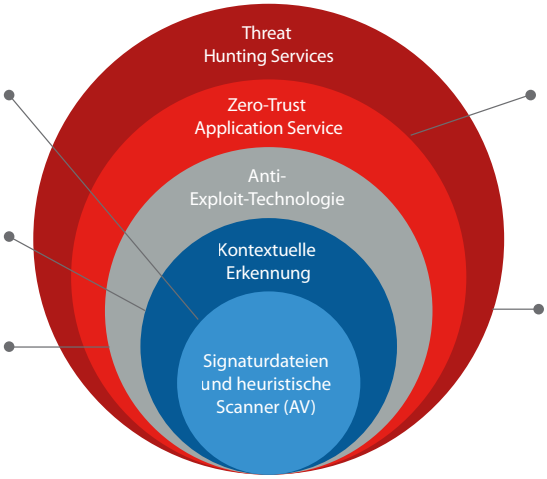
Zero-Trust-Modell: Mehrschichtiger Schutz

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
Erkennen Sie gefährdete Endpoints, Angriffe in der Frühphase und verdächtige Aktivitäten und identifizieren Sie IoAs, die die

LEISTUNGSSTARKE, VEREINFACHTE SICHERHEIT MIT DER UNIFIED SECURITY PLATFORM VON WATCHGUARD

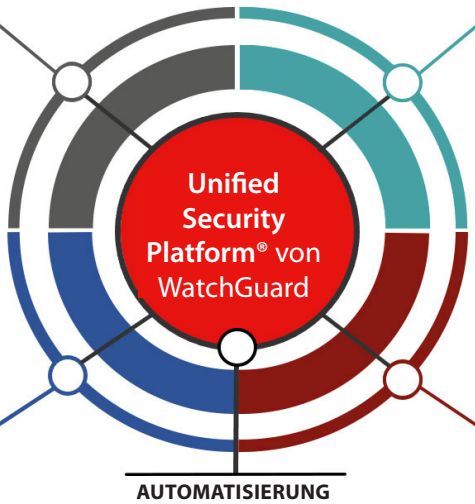
Die Unified Security Platform-Architektur von WatchGuard bietet eine einzige Plattform für die Bereitstellung moderner Sicherheitsmaßnahmen. Mit unserem Plattformansatz können Sie leistungsstarke Sicherheitsdienste für sämtliche Bedrohungsvektoren bereitstellen und dabei gleichzeitig die betriebliche Effizienz und die Rentabilität steigern.

UMFASSENDE SICHERHEIT

Ein umfassendes Portfolio aus Produkten und Services für **Endpoint-Sicherheit, Multifaktor-Authentifizierung und Netzwerksicherheit** zum Schutz von Umgebungen, Anwendern und Geräten.

TRANSPARENZ UND KONTROLLE

Zentralisierte Sicherheitsverwaltung, Transparenz und erweitertes Reporting über **WatchGuard Cloud.**



BETRIEBLICHE AUSRICHTUNG

Vereinfachte Geschäftsabläufe mit direktem API-Zugang, einer umfangreichen Auswahl an sofort einsatzbereiten **Integrationen** und Unterstützung für alle Zahlungs- und Verbrauchsmodelle über **FlexPay.**

KOLLEKTIVE INTELLIGENZ

Eine umfassend integrierte Plattform zur Einführung eines Zero trust-Sicherheitskonzepts über das **Identity Framework** von WatchGuard und zur Bereitstellung eines echten XDR-basierten Ansatzes für Bedrohungserkennung und -beseitigung über **ThreatSync®**.

AUTOMATISIERUNG

Automation Core® von WatchGuard ermöglicht die Vereinfachung und Skalierung sämtlicher Aspekte der Nutzung, Bereitstellung und Verwaltung von Sicherheitsservices.

Unterstützte Plattformen und Systemanforderungen von WatchGuard EPDR

Unterstützte Betriebssysteme: Windows (Intel und ARM), macOS (Intel und ARM), Linux, iOS und Android.

Unterstützung von älteren Systemen ab Windows XP SP3 und Server 2003.

EDR-Funktionen sind unter Windows, macOS und Linux verfügbar, wobei Windows sämtliche Funktionen uneingeschränkt unterstützt.

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Safari und Microsoft Edge.

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