

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.

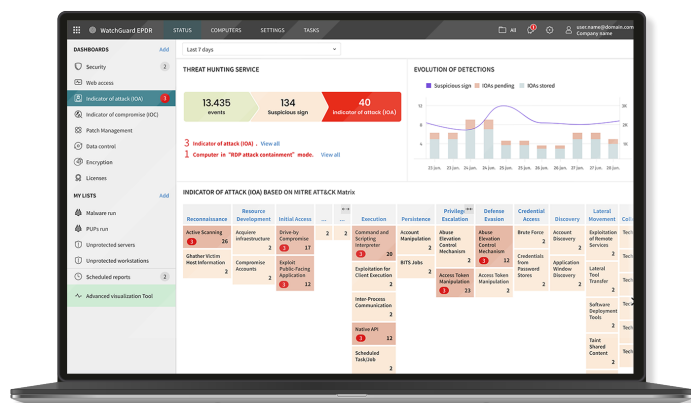
Traditionelle, auf Vorbeugung ausgerichtete Technologien für Endpoint-Schutz sind für bekannte Bedrohungen und böswillige Verhaltensweisen geeignet, bieten jedoch keinen ausreichenden Schutz vor modernen Cyberbedrohungen.

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 diese Lösung eine sehr breite Palette an Technologien zum Endpoint-Schutz, basierend auf selbstlernender KI und kontextbasierter Verhaltensanalyse 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 integriert Virenschutz der nächsten Generation mit selbstlernenden, KI-gestützten Analysen und fortschrittlichen EDR-Technologien in einer einzigen Lösung, sodass IT-Teams mit fortschrittlichen Cyber-Bedrohungen umgehen können:

Virenschutz-Technologien der nächsten Generation und Hardening-Technologien

- Firewall, IDS und Gerätekontrolle
- KI-gestützte Verhaltensanalysen gegen Ransomware-, Phishing-, dateilose und malwarefreie Angriffe
- Kollektive Intelligenz und Heuristik vor der Ausführung
- Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Manipulationsabwehr, Web-/URL-Filterung und Schutz vor Phishing-Angriffen
- Automatische Behebung und Rollback
- Wiederherstellung verschlüsselter Dateien (Schattenkopien)
- Schwachstellenanalyse

Neuartige Sicherheitstechnologien

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Selbstlernende KI mit kontextbezogener Verhaltensanalyse zur Erkennung und Abwehr von dateilosen und Living-off-the-Land-Angriffen (LotL)
- Cloud-basierte KI, die 100 % der Prozesse (APTs, Ransomware, Rootkits usw.) klassifiziert und versteckte Bedrohungen in Echtzeit blockiert
- Cloud-Sandboxing in realen Umgebungen
- Schutz vor Exploits Schutz vor Netzwerkangriffen, bei denen Schwachstellen in über das Internet zugänglichen Diensten ausgenutzt werden
- Threat Hunting mit Verhaltensanalyse und Erkennung von Angriffsindikatoren (IoAs) für LotL-Angriffe, wobei IoAs dem MITRE ATT&CK Framework entsprechen
- Kontinuierliche Auswertung von Verbindungen zwischen Endpoints, um seitliche Bewegungen mit Endpoint Access Enforcement zu blockieren
- Erkennung und Prävention von RDP-Angriffen Isolierung von Endpoints

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 Erfolgchancen 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

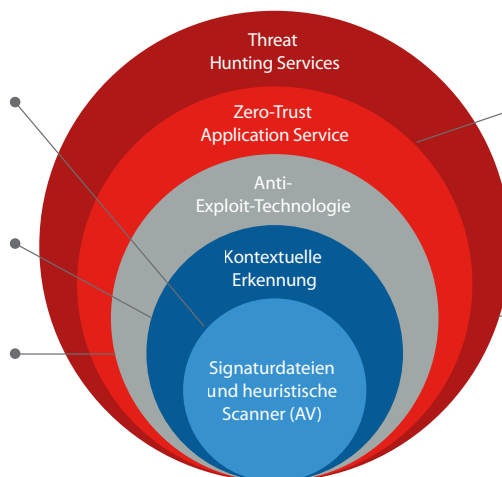
Effektive, optimierte Technologie zur Erkennung bekannter Angriffe

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

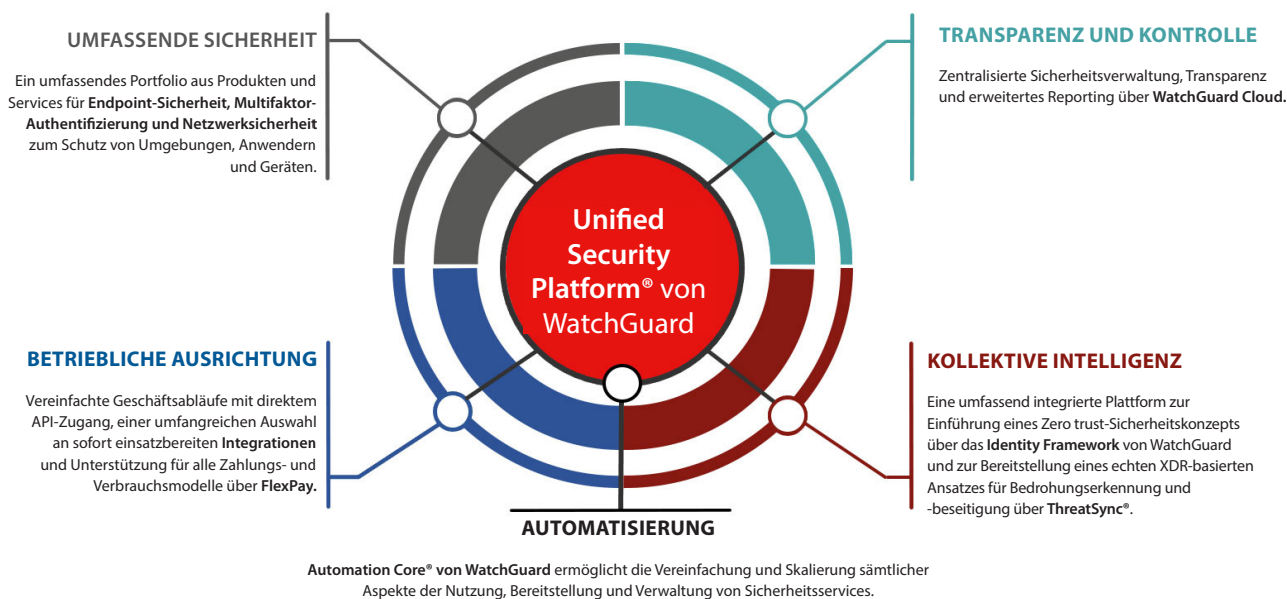
Erkennt, ob auf einer vorherigen Ebene ein Verstoß vorliegt, stoppt Angriffe auf bereits infizierten Computern und verhindert laterale Bewegungsangriffe innerhalb des Netzwerks

Ebene 5/Threat Hunting Service

Erkennen Sie kompromittierte Endpoints, Angriffe im Frühstadium und verdächtige Aktivitäten und identifizieren Sie IoAs, die die Erkennungs- und Reaktionszeit (MTTD und MTTR) minimieren.

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.



Unterstützte Plattformen und Systemanforderungen von WatchGuard EPDR

Unterstützte Betriebssysteme: [Windows \(Intel und ARM\)](#), [macOS \(Intel und ARM\)](#), [Linux](#), [iOS](#) und [Android](#).

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](#).