DATENBLATT | SOC

WATCHGUARD ADVANCED EPDR

HERAUSFORDERUNGEN BEI DER CYBERSICHERHEIT

Endpoints sind das primäre Ziel der meisten Cyberangriffe. Da die Technologieinfrastruktur immer komplexer wird, fällt es Unternehmen schwer, das nötige Fachwissen für die Überwachung und Verwaltung von Endpoint-Sicherheitsrisiken zu finden. Welche Arten von Herausforderungen müssen Sicherheitsteams bewältigen, wenn sie Endpoint-Sicherheitslösungen einsetzen?

- **Sich ständig verändernde, komplexe Bedrohungen:** Effiziente, proaktive Sicherheitspraktiken können den Unterschied zwischen einem kleinen Sicherheitsvorgehen und der Rolle als Opfer ausmachen. Diese Praktiken reichen von der Reduzierung der Angriffsoberfläche bis zum Erkennen sich entwickelnder Bedrohungen, bevor es zu einer tatsächlichen Kompromittierung kommt.
- **Alarmmüdigkeit, fehlende Effizienz:** Unternehmen erhalten pro Woche Tausende von Warnmeldungen, von denen nur 19 % als vertrauenswürdig eingestuft und nur 4 % geprüft werden. Sicherheitsteams verbringen zwei Drittel der Zeit mit der Verwaltung von Warnmeldungen und der manuellen Klassifizierung verdächtiger Dateien.
- **Schlechte Performance:** Häufig erfordern Lösungen für Endpoint-Sicherheit die Installation und Verwaltung mehrerer Agenten auf jedem überwachten Computer, Server und Laptop. Dies verursacht schwerwiegende Fehler, eine schlechte Performance und einen hohen Ressourcenverbrauch.

Zur Verteidigung benötigen Sicherheitsteams **autonome Präventions-, Erkennungs- und Reaktionslösungen** sowie entsprechende **Mittel, damit sie Bedrohungen, die in Umgebungen lauern, leicht aufspüren und darauf reagieren** sowie die Sicherheitsstruktur weiter optimieren können, um die Verweildauer von Angreifern zu minimieren.

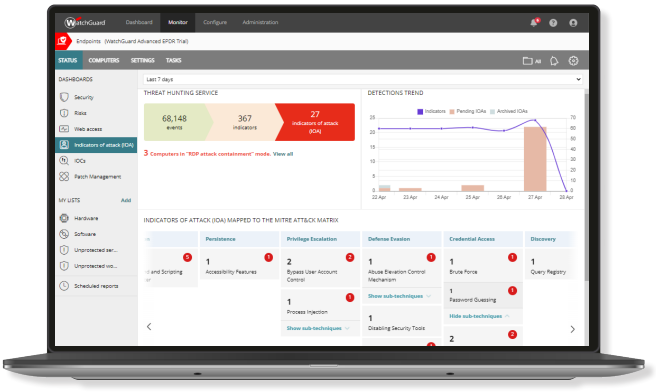
VERBESSERN SIE IHRE CYBERSICHERHEITSDIENSTE

WatchGuard Advanced EPDR ist eine hochmoderne Cybersicherheitslösung, die über die Cloud für Computer, Laptops und Server bereitgestellt wird. Sie automatisiert die Prävention, Erkennung und Eindämmung von fortschrittlichen Bedrohungen sowie die Reaktion darauf innerhalb und außerhalb des Unternehmensnetzwerks.

Sie kombiniert vorbeugende und EDR-Technologien mit zwei Sicherheitsservices:

- **Zero-Trust Application Service:** Cloud-basiertes maschinelles Lernen klassifiziert automatisch alle Dateien
- **Threat Hunting Service:** Verhaltensanalyse zur Aufdeckung von Bedrohungsakteuren, die Living-Off-The-Land (LOTL)-Techniken verwenden.

WatchGuard Advanced EPDR erweitert WatchGuard EPDR um Hunting Tools wie die IOCs-Suchmaschine, erweiterte IOAs-Erkennungen, die auf MITRE ATT&CK abgebildet werden, und Fernzugriff auf Endpoints für schnelle Untersuchung und Reaktion.



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

WatchGuard Advanced EPDR vereint herkömmliche Endpoint-Technologien mit EDR-Technologien in einer einzigen Lösung und ermöglicht IT-Fachkräften, gegen fortgeschrittene Cyberbedrohungen vorzugehen.

Werkzeuge zur Reduzierung der Angriffsfläche

- Zentralisierte Erkennung und Bewertung von Endpoint-Sicherheitsrisiken
- Proaktive Erkennung nicht verwalteter Endpoints
- Bewertung der Schwachstellen von Betriebssystemen und Hunderten von Anwendungen

Herkömmliche Präventionsmethoden

- Persönliche oder verwaltete Firewall (IDS)
- Gerätesteuerung
- Anwendungskontrolle: Deny-Liste / Allow-Liste
- Ständige Multi-Vektor-Scans zur Malware-Erkennung, auch on-Demand
- Vorab-Ausführungs-Heuristik
- URL Filtering – Webbrowsing
- Phishingschutz und Manipulationsabwehr
- Erkennung von Angriffen durch Analyse des Netzwerkverkehrs
- Automatische Behebung und Möglichkeit für Rollbacks
- Verschlüsselte Dateien über Schattenkopien wiederherstellen

Hunting- und Erkennungstechnologien

- Ständige Überwachung der Endpoint-Aktivität mit EDR
- Zero-Trust Application und Threat Hunting Services
- Sandboxing in realen Umgebungen
- Schutz vor Exploits
- Angriffsindikatoren (IoA) werden MITRE ATT&CK zugeordnet
- Automatisierte Erkennung und Eindämmung von RDP-Angriffen
- Suche nach STIX-Angriffsindikatoren (IOC) und YARA-Regeln
- Verhinderung der Ausführung gängiger Angriffstechniken mit erweiterten Sicherheitsrichtlinien

Werkzeuge zur Eindämmung und Abhilfe

- Computerisolierung und Neustart von Systemen
- Remote-Shell aus der Cloud zu Endpoints

VORTEILE

Kosteneffizienter Betrieb – keine Zeitverschwendung mehr für verdächtige Dateien
Wie WatchGuard EPDR gibt der Zero-Trust Application Service Ihrem Team die Zeit zurück, die es für das Reverse-Engineering verdächtiger Dateien aufgewendet hat, vor denen andere Lösungen warnen, ohne den Prüfprozess zu schließen und die letzte Entscheidung Ihnen zu überlassen.

Umfassende Endpoint-Sicherheit, die sich an Ihre Dienste anpassen lässt
WatchGuard Advanced EPDR bietet eine umfassende Palette von Funktionen zur Stärkung von Endpoint-Sicherheitsprogrammen, einschließlich Reduzierung der Angriffsfläche, Bedrohungsvorbeugung, -erkennung und -reaktion, proaktive Hunting-Werkzeuge und Remote-Endpoint-Verbindung für eine schnelle Reaktion.

Verbesserte Suche und Reaktion per Mausklick
Dank zentralisierter IOC-Suchen können WatchGuard Advanced EPDR-Sicherheitsteams Bedrohungen erkennen, ohne sich mit komplexen Abfragen befassen zu müssen. Der Threat Hunting Service liefert kontextualisierte IOA mit Telemetrie zur weiteren Untersuchung.

Skalierbare Managed Security Services, passend zu Ihrem Wachstumstempo

Die Unified Security Platform-Architektur von WatchGuard
bietet umfassende Sicherheit vom Netzwerk bis zu Endpoints, WLAN und Identität mit unvergleichlichen Plattformfunktionen ohne zusätzliche Kosten. Je mehr Services Sie übernehmen, desto größer sind Ihre betrieblichen und geschäftlichen Vorteile.

ZERO-TRUST-MODELL: MEHRSCHICHTIGER SCHUTZ

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

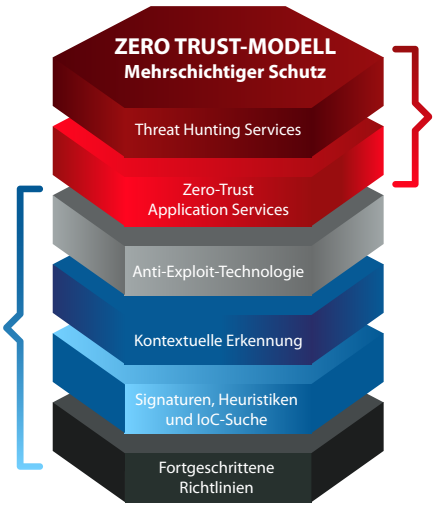
ENDPOINT-EBENEN:

Ebene 1/Verbesserte Sicherheitsrichtlinien
Erkennen oder Blockieren der Ausführung verbreiteter Angriffstechniken

Ebene 2/Signaturdateien, heuristische Technologien und STIX IOC-Suchmaschine
ermöglichen Sicherheitsteams die Suche nach kürzlich bekannt gewordenen Angriffen anhand von Hash, Dateinamen, Pfad, C2-Domäne, IP und YARA-Regeln

Ebene 3/Kontextuelle Erkennung von Angriffen ohne Malware mit Betriebssystem-Werkzeugen wie PowerShell, WMI, Webbrowsern und anderen häufig angegriffenen Anwendungen wie Java, Adobe und anderen.

Ebene 4/Anti-Exploit-Technologie
Erkennung dateiloser Angriffe, die Schwachstellen ausnutzen



CLOUDNATIVE EBENEN

Ebene 5/Zero-Trust Application Service
Klassifiziert jeden einzelnen Prozess, bevor er ausgeführt wird, wobei jede Ausführung abgelehnt wird, solange sie nicht als vertrauenswürdig zertifiziert wurde.

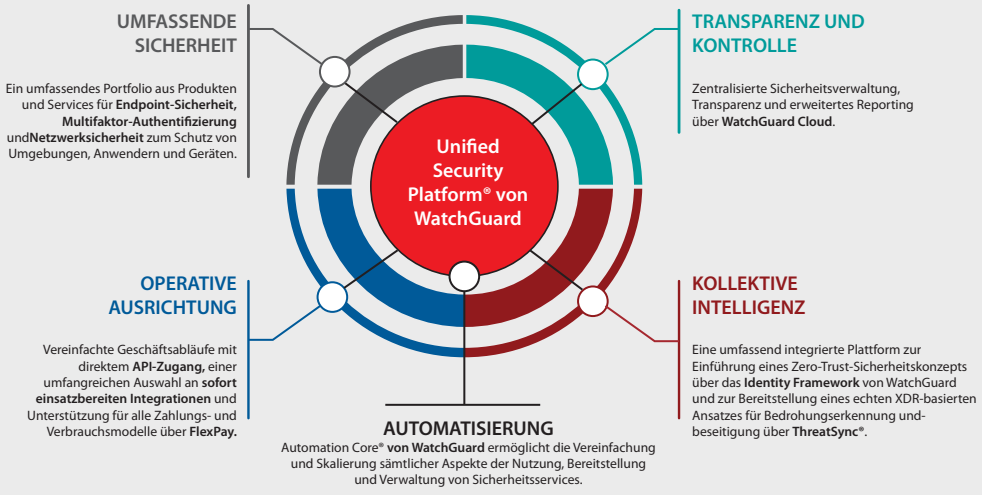
Ebene 6/Threat Hunting Service
Erkennung von angegriffenen Endpoints, frühen Phasen eines Angriffs, verdächtigen Aktivitäten und IoA. Nicht-deterministische IOA werden in der Cloud-basierten Konsole mit den zugehörigen Ereignissen kontextualisiert, sodass Sicherheitsanalysten potenzielle Angriffsversuche untersuchen können.

LEISTUNGSSTARKE, VEREINFACHTE SICHERHEIT MIT DER UNIFIED SECURITY PLATFORM VON WATCHGUARD

Die WatchGuard Unified Security Platform-Architektur 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. Hier erfahren Sie mehr.

Eine einzige, skalierbare Plattform zur Verbesserung moderner Sicherheitslösungen.



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