Warum Sie WatchGuard Endpoint Security kaufen sollten

WatchGuard EPDR bietet das ultimative Sicherheitspaket für Endpoints, das Virenschutz der nächsten Generation mit EDR-Funktionen kombiniert. Dazu gehört der einzigartige Zero-Trust Application Service, der die Legitimität und Sicherheit aller ausgeführten Anwendungen dank einer Kombination aus automatisierten, KI-gesteuerten Prozessen und Threat Hunting-Diensten zur Erkennung von böswilligen Akteuren und Insidern zertifiziert.

WatchGuard EPDR bietet XDR-Funktionen, und in Kombination mit der produktübergreifenden Korrelation, die unsere Unified Security Platform-Architektur bietet, steigert die Lösung die hohe Transparenz und Sicherheitseffizienz gegen komplexe Angriffe.

Warum Unternehmen sich für WatchGuard EPDR entscheiden

WatchGuard EPDR nutzt nicht nur eine einzige Technologie, sondern verschiedene, um die Erfolgschancen von Angreifern zu reduzieren. Durch das Zusammenspiel der folgenden Technologien wird das Risiko eines Angriffs minimiert:

Ebene 1/Signaturdateien und heuristische Technologien

Effektive, optimierte Technologie zur Erkennung bekannter Angriffe

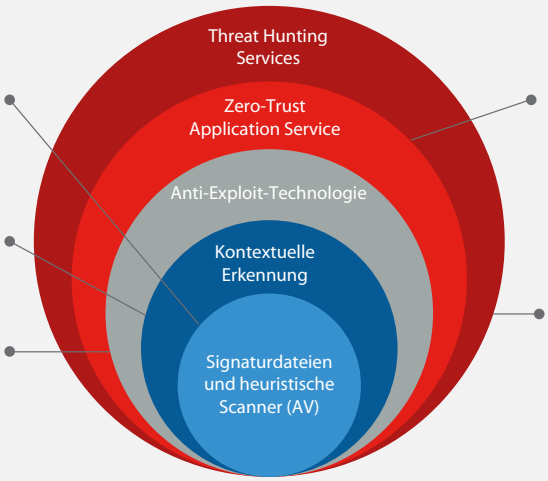
Ebene 2/Kontextuelle Erkennung

Erkennung von datei- und malwarefreie Angriffen

Ebene 3/Anti-Exploit-Technologie

Erkennung dateiloser Angriffe, die Schwachstellen ausnutzen

Zero Trust-Modell: Mehrschichtiger Schutz



Ebene 4/Zero-Trust Application Service

Klassifiziert jeden einzelnen Prozess, wobei standardmäßig jede Ausführung abgelehnt wird, solange sie nicht als vertrauenswürdig zertifiziert wurde. Bedrohungen müssen nicht manuell klassifiziert oder an Sicherheitsadministratoren übergeben werden.

Ebene 5/Threat Hunting Service

Erkennung von gefährdeten Endpoints, Angriffen im Frühstadium, verdächtigen Aktivitäten und Identifizierung von IoAs zur Minimierung der Erkennungs- und Reaktionszeit (MTTD und MTTR)

Wichtige Endpoint-Sicherheitsfunktionen

ENDPOINT-SICHERHEIT UND -MANAGEMENT

Schutz
Schutz vor bekannter und Zero-Day-Malware, Ransomware und Exploits
Traditioneller Schutz mit generischen und optimierten Signaturen
Schutz vor Advanced Persistent Threats (APT)
Zero-Trust Application Service: Maschinelles Lernen zur Klassifizierung sämtlicher Prozesse
Threat Hunting: Verhaltensanalyse und Erkennung von Angriffsindikatoren (IoA)
Persönliche und verwaltete Firewall
IDS/HIPS
Schutz vor Netzwerkangriffen
URL Filtering, Webbrowsing und Anti-Phishing
Monitoring
Risk-Monitoring für Endpoints
Schwachstellenanalyse
Zero-Trust Application Service
Zwölfmonatige Datenaufbewahrung für die rückwirkende Untersuchung von Angriffen

Erkennung
Erkennung von kompromittierten vertrauenswürdigen Anwendungen
Zero-Trust Application Service
Vollständig konfigurierbare und sofortige Warnmeldungen für Sicherheitsrisiken
Eindämmung
Computerisolierung und Programmblockierung
Reaktion und Abhilfemaßnahmen
Fähigkeit, die von Angreifern durchgeführten Aktionen rückgängig zu machen und zu beheben
Zentralisierte Quarantäne
Automatische Analyse und Desinfektion
Schattenkopien
Fähigkeit, unbekannte und unerwünschte Anwendungen zu blockieren
Untersuchung
Threat Hunting Service: Deterministische Indikatoren, zugeordnet zu MITRE ATT&CK
Threat Hunting Service: Nicht-deterministische Indikatoren, zugeordnet zu MITRE ATT&CK mit kontextbezogener Telemetrie
Ereignisdiagramme und Lebenszyklusinformationen über die Web-Konsole verfügbar
Möglichkeit des Exports von Lebenszyklusinformationen für lokale Analysen
Advanced Reporting Tool (Add-on)
Erweiterte Angriffsuntersuchung (Jupyter Notebooks)

Reduzierung der Angriffsfläche
Sperrmodus im Rahmen des erweiterten Schutzes
Anti-Exploit-Technologie
Internetschutz
Gerätesteuerung
Automatische Aktualisierung und Erkennung ungeschützter Endpoints
Patch-Management für Betriebssysteme und Anwendungen von Drittanbietern
Sicherheit für VPN-Verbindungen (erfordert WatchGuard Firebox)
Sicherer Zugang zum WLAN-Netzwerk über Access Points
Add-ons
WatchGuard Data Control
WatchGuard Advanced Reporting
WatchGuard Patch Management
WatchGuard Full Encryption
WatchGuard SIEMFeeder
Unterstützte Plattformen
Windows Intel und Windows ARM
macOS Intel und macOS ARM (M1 & M2)
Linux
Android- und iOS-Geräte
Virtuelle Umgebungen – persistent und nicht persistent (VDI)

Verlassen Sie sich nicht nur auf das, was wir sagen.

„Da Cyberangriffe auf Endpoints immer weiter zunehmen, sind unsere Kunden zunehmend darauf angewiesen, dass wir ihnen bei der Erfüllung ihrer Sicherheitsanforderungen helfen. Die Kombination der WatchGuard Cloud mit dem Endpoint Security-Portfolio ermöglicht uns nicht nur, diesen Schutz anzubieten, sondern auch, unser Angebot an Sicherheitsdienstleistungen zu erweitern, die Effektivität und Effizienz zu steigern und das Geschäft auszubauen.“

– Bill Walter, Partner
Gross, Mendelsohn & Associates