DATENBLATT

WatchGuard Endpoint für Server

Maßgeschneiderter Schutz für kritische Infrastrukturen

Schutz des Kerns der modernen Infrastruktur

Server sind das Rückgrat jedes Unternehmens. Auf ihnen werden sensible Daten gespeichert und sie sorgen dafür, dass kritische Geschäftsanwendungen reibungslos funktionieren. Sie sind jedoch auch Hauptziele für Angriffe durch Ransomware, laterale Bewegungen und die Eskalation von Berechtigungen. Herkömmlicher Endpoint-Schutz ist nicht für Server Workloads optimiert, die kontinuierliche Verfügbarkeit, eine minimale Latenz und ressourceneffiziente Sicherheit erfordern. Unternehmen benötigen einen dedizierten, kontinuierlichen Schutz, der speziell für den Schutz ihrer Infrastruktur entwickelt wurde, ohne die Leistung zu beeinträchtigen.

Schutz kritischer Infrastrukturen

Wenn Unternehmen ihre IT-Umgebungen weiterentwickeln, werden die Schutzanforderungen immer komplexer. Aufgrund hybrider und Multi-Cloud-Architekturen müssen Sicherheitsteams oft zwischen unterschiedlichen Tools wechseln, was zu eingeschränkter Transparenz und inkonsistentem Schutz führt. Legacy-Lösungen können mit heutigen Schutzanforderungen nicht Schritt halten und führen zu Leistungsengpässen, Sicherheitslücken und einem fehlenden ROI für Infrastrukturinvestitionen.

Mit WatchGuard Endpoint Security für Server können Sie diese Herausforderungen direkt meistern, da die Lösung einheitliche Transparenz, intelligenten Schutz und vereinfachte Verwaltung über alle Workloads hinweg bietet. Sie basiert auf der WatchGuard Endpoint Security Platform und bietet einen zentralen Überblick über Ihre gesamte Infrastruktur, darunter auch virtuelle Maschinen, Endpoints und Workloads.

Die Agenten werden nahtlos über physische und virtuelle Server (On-Premise oder in AWS, Azure und Google Cloud) bereitgestellt und fungieren als Durchsetzungspunkte, die von derselben Multi-Tenant-Konsole wie Workstations und mobile Geräte verwaltet werden. Die flexible, rollenbasierte Verwaltung passt sich an die Struktur Ihres Unternehmens an und sorgt für ein optimiertes, sicheres Management.

Mit selbstlernender KI und kontextbasierter Verhaltensanalyse kombiniert Endpoint Security für Server das breiteste Spektrum an Endpoint-Schutztechnologien mit automatisierter Erkennung und Reaktion. Dies ermöglicht eine schnellere Erkennung neuer Angriffe und eine intelligentere, automatisierte Behebung von Problemen, ohne dass Leistung oder Benutzerfreundlichkeit beeinträchtigt werden.

WatchGuard für Server integriert Virenschutz der nächsten Generation mit selbstlernenden, KI-gestützten Analysen und fortschrittlichen EDR-Technologien in einer einzigen Lösung, sodass IT-Teams fortschrittliche Cyber-Bedrohungen abwehren können:

Virenschutz und Sicherungstechnologie der nächsten Generation

- 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)
- Cloudbasierte 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 von RDP-Angriffen und Vorbeugung
- Eindämmungs- und Abhilfemöglichkeiten, wie Computerisolierung und Programmblockierung

Erweiterte Erkennung und Reaktion, speziell für Server

WatchGuard Endpoint Security für Server bietet die gleichen erweiterten Funktionen zur Bedrohungserkennung und -reaktion wie unser Schutz für Workstations, mit zusätzlicher Data Intelligence für Server Workloads. Die KI-gesteuerte Verhaltensanalyse überwacht jeden Prozess, jede Verbindung und jede Datei in Echtzeit, um Bedrohungen zu erkennen und zu blockieren, bevor sie sich ausbreiten oder eskalieren.

Verhinderung von Exploits und Schwachstellenmanagement

Ungepatchte oder veraltete Software macht Server oft zu einfachen Zielen. Die Exploit Prevention Engine von WatchGuard identifiziert und blockiert Exploit-Versuche, während die dynamischen Tools zur Reduzierung der Angriffsfläche, einschließlich der integrierten Firewall, der integrierten Schwachstellenbewertung und der Gerätekontrolle, Administratoren dabei helfen, Sicherheitslücken schnell zu priorisieren und zu beheben.

Intelligenterer Schutz, stärkere Leistung

Server Workloads erfordern sowohl Geschwindigkeit als auch Ausfallsicherheit. Die leichten, ressourcenbewussten Agents von WatchGuard sind optimiert, um die Latenz zu minimieren und die Anwendungsleistung zu erhalten und gleichzeitig einen leistungsstarken, KI-gesteuerten Schutz aufrechtzuerhalten. Jeder Agent lernt kontinuierlich aus der globalen Telemetrie und verwendet in der Cloud trainierte Modelle, um das Verhalten zu analysieren und Bedrohungen in Millisekunden zu erkennen – sogar offline. Diese kontinuierliche Selbstlernschleife sorgt für eine schnellere Erkennung, eine intelligentere Reaktion und einen sich weiterentwickelnden Schutz, der von Tag zu Tag stärker wird – ohne die Verfügbarkeit oder die Benutzererfahrung zu beeinträchtigen.

Ein mehrschichtiger Ansatz

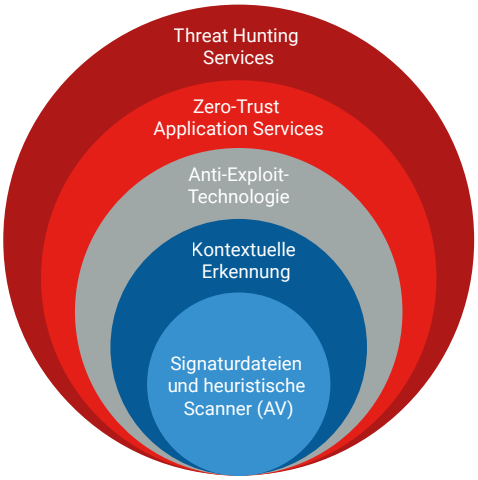
Endpoint Security für Server von WatchGuard basiert nicht nur auf einer einzigen Technologie. Sie kombiniert mehrere Technologien miteinander, um die Erfolgschancen von Angreifern zu reduzieren und das Risiko von Sicherheitsverletzungen zu minimieren. Dazu gehört unser einzigartiger Zero-Trust Application Service, der automatisch 100 % der Anwendungen und Prozesse klassifiziert, bevor sie ausgeführt werden.

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



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

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit des Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security and Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von über 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter watchguard.de.

Deutschland, Österreich, Schweiz +49 206 596 1001 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.