WatchGuard Endpoint-Sicherheit

Erweiterbarer Schutz zur Vorbeugung und Erkennung sowie zur Reaktion auf fortgeschrittene Bedrohungen

Der Endpoint hat eine Vielzahl bekannter Schwachstellen, die sich ausnutzen lassen. Außerdem sind häufig veraltete Softwareversionen installiert. Das macht ihn zu einem beliebten Ziel von Cyberkriminellen. Im Internet sind diese Geräte oft nicht durch Sicherheitsmaßnahmen auf Ebene des Unternehmensperimeters geschützt. Mitarbeiter können Hackern bisweilen sogar unwissentlich den Zugang zu den Endpoints und Netzwerken des Unternehmens ermöglichen. Heute müssen Unternehmen aller Größenordnungen keine leistungsstarke Endpoint-Security mehr implementieren, die in fortschrittliche Endpoint-Detection-and-Response-(EDR)-Technologien integrierte Endpoint Protection (EPP) umfasst.

Die Endpoint-Sicherheitsplattform von WatchGuard bietet maximalen Schutz bei minimaler Komplexität und macht damit Schluss mit Unsicherheiten bei der Endpoint-Security. Unsere anwenderzentrierten Sicherheitsprodukte und -dienste bieten fortschrittliche EPP- und EDR-Ansätze mit einem Komplettpaket von Sicherheits- und Betriebstools. Sie schützen Personen, Geräte und die Netzwerke, mit denen sie sich verbinden, vor bösartigen Websites, Malware, Spam und anderen gezielten Angriffen. Unsere WatchGuard EPDR- und WatchGuard EDR-Produkte werden durch automatisierte, KI-gesteuerte Prozesse und von Sicherheitsanalysten durchgeführte Investigationsservices gestützt und bieten Threat Hunting Services und eine 100-prozentige Klassifizierung von Anwendungen. Dies bestätigt die Legitimität und Sicherheit aller ausgeführten Anwendungen, eine entscheidende Notwendigkeit für jedes Unternehmen, das ein Zero-Trust-Sicherheitsmodell implementiert.

Gut oder schädlich? Zu 100 Prozent verlässlich

Die meisten Endpoint-Sicherheitsprodukte blockieren, was als schädlich bekannt ist, untersuchen, was verdächtig ist, und lassen zu, was nicht bekannt ist. Sie ermöglichen damit Malware, die sich schnell verändert, die Abwehr zusammen mit anderem unbekannten Datenverkehr zu umgehen. Die Produkte WatchGuard EDR und WatchGuard EPDR bieten dagegen einen Zero Trust Application Service, der ausführbare Dateien 100-prozentig klassifiziert. Dazu analysiert er alle verdächtigen und unbekannten Prozesse und Anwendungen mithilfe spezieller Algorithmen für maschinelles Lernen in unserer Cloudplattform und verifiziert sie bei Bedarf sogar mit unseren Labortechnikern. Alle ausführbaren Dateien werden als „Goodware“ oder „Malware“ eingestuft, so dass Kunden nur bestätigte Warnmeldungen erhalten. Darüber hinaus genießen sie den ultimativen Schutz, der sich daraus ergibt, dass die Standardeinstellung in einem Zero-Trust-Modell die Ablehnung ist.

Lauernde Bedrohungen finden, ohne zusätzliches Personal

Threat Hunting erfordert in der Regel hochqualifizierte Ressourcen und nimmt viele Stunden in Anspruch, bevor Bedrohungen aufgespürt und Erkenntnisse gewonnen werden, die aufzeigen, wie man dieser Bedrohungen Herr werden kann. Unsere fortschrittlichen EDR-Lösungen bieten einen Threat Hunting Service, bei dem unsere Sicherheitsanalysten die Endpoint-Umgebung des Kunden überwachen und Informationen über potenzielle laufende Angriffe bereitstellen. Dazu gehören eine Ursachenanalyse, festgestellte Anomalien, relevante IT-Erkenntnisse und Pläne zur Reduzierung der Angriffsfläche. Dies ist eine Standardfunktion unserer Produkte WatchGuard EDR und WatchGuard EPDR. IT-Mitarbeiter brauchen deshalb für die Untersuchung infizierter Endpoints keine Zeit und Energie mehr aufzuwenden.

Die Vorteile von intuitivem cloud-basiertem Management

Unternehmen mit wenigen IT-Mitarbeitern und geringem Sicherheits-Know-how profitieren von WatchGuard Cloud. Diese cloud-basierte Verwaltungsplattform macht die Bereitstellung, Konfiguration und Verwaltung Ihrer Endpoint-Sicherheitsprodukte zum Kinderspiel. Sie bietet Echtzeitschutz und -kommunikation mit Endpoints, einschließlich unserer Sicherheits-Engine und Signaturen sowie URL Filtering-Funktionen, mit deren Hilfe Anwender Aufgaben und Konfigurationen in wenigen Sekunden an Tausende von Computern senden können. Darüber hinaus ermöglicht WatchGuard Cloud die Verwaltung des gesamten Portfolios in einer einzigen Oberfläche, was Infrastrukturkosten senkt und den Zeitaufwand für Berichterstellung und betriebliche Aufgaben minimiert.

Erweiterung der Sicherheits-, Transparenz- und Einsatzfähigkeiten

Optionale Module sind mit allen EPP- und EDR-Sicherheitsprodukten erhältlich. Fügen Sie Patch Management hinzu, um Updates und Patches für Betriebssysteme für Drittanbieteranwendungen und nicht unterstützte (EOL-) Softwareprogramme zentral zu verwalten. Stellen Sie Full Encryption bereit, um Endpoint-Informationen zu verschlüsseln und zu entschlüsseln. Nutzen Sie unser Advanced Reporting Tool, um Sicherheitsinformationen zu erzeugen und Angriffe und ungewöhnliches Verhalten zu identifizieren. Entscheiden Sie sich für Data Control, um unstrukturierte personenbezogene Daten, die an Endpoints gespeichert sind, zu entdecken, zu klassifizieren, zu prüfen und zu überwachen. SIEM Feeder erzeugt eine neue Quelle für wichtige Details, die alle auf Ihren Geräten ausgeführten Prozesse überwacht. Systems Management, unser RMM-Tool, dient der Verwaltung, Überwachung und Wartung Ihrer gesamten IT-Infrastruktur.

Ein Komplettpaket mit flexiblen Optionen für jeden Bedarf

WatchGuard EDR und WatchGuard EPDR

- Bietet leistungsstarken Endpoint Detection and Response (EDR)-Schutz vor Zero-Day-Angriffen, Ransomware, Cryptojacking und anderen fortschrittlichen gezielten Angriffen. Genutzt werden hierbei neue und neu entstehende KI-Modelle für maschinelles Lernen und Deep Learning.
- Zur Auswahl stehen Optionen nur für EDR (WatchGuard EDR) sowie für EPP + EDR (WatchGuard EPDR).

  100-prozentige Klassifizierung mit dem Zero-Trust Application Service – zur Erstellung der Art von Reaktion, die für die Einführung eines Zero-Trust-Modells erforderlich ist

  Optimierung von Einsatz und Effizienz des Personals dank Erkenntnissen aus dem Threat Hunting Service.
- Implementierung einer umfassenden Endpoint-Security mit WatchGuard EPDR, das alle Vorteile unseres WatchGuard-Produkts zur Endpoint Detection and Response und unseres Endpoint-Sicherheitsprodukts in einem Paket enthält.

WatchGuard EPP

- Schützt Endpoints vor Viren, Malware, Spyware und Phishing mit Signaturen, lokalem Cache und sogar unseren eigenen proprietären Intelligence-Feeds, die aus der zuvor durch WatchGuard EDR und WatchGuard EPDR erkannten Malware stammen.
- WatchGuard wurde für Unternehmen entwickelt, die viele verschiedene Geräte unterstützen. WatchGuard EPP zentralisiert den Antivirenschutz der nächsten Generation für all Ihre Desktop-PCs, Laptops und Server mit Windows, MacOS und Linux sowie für die führenden Virtualisierungssysteme und Android & iOS-Geräte. Unsere Lösung ermöglicht es Ihnen, die Sicherheit und Vertraulichkeit der auf den Android & iOS-Smartphones und -Tablets von Anwendern gespeicherten Daten zentral zu verwalten.
- Findet Zero-Day-Angriffe durch den Einsatz von Verhaltensheuristiken und bekannten Indikatoren für Angriffe als „kontextbezogene Regeln".

Zusätzliche Sicherheitsmodule

Fügen Sie optionale Module hinzu, die mit allen EPP- und EDR-Sicherheitsprodukten erhältlich sind:

WatchGuard Patch Management

WatchGuard Patch Management ist eine Lösung zur zentralen Verwaltung von Updates und Patches für Betriebssysteme und für Hunderte von Drittanbieteranwendungen und nicht unterstützte Software-Programme (EOL).

WatchGuard Full Encryption

WatchGuard Full Encryption nutzt die BitLocker-Technologie von Microsoft zur Ver- und Entschlüsselung von Endpoint-Informationen, wobei die Wiederherstellungsschlüssel über unsere cloudbasierte Management-Plattform zentral verwaltet werden.

Erweitern Sie mit zusätzlichen optionalen Modulen, die nur bei WatchGuard EPDR- und WatchGuard EDR-Sicherheitsprodukten verfügbar sind:

WatchGuard Advanced Reporting Tool

WatchGuard Advanced Reporting Tool generiert automatisch Sicherheitsinformationen und stellt Tools bereit, mit denen Angriffe, ungewöhnliche Verhaltensmuster sowie interner Missbrauch des Firmennetzwerks erkannt werden können.

WatchGuared Data Control*

WatchGuared Data Control* erkennt, klassifiziert, prüft und überwacht unstrukturierte personenbezogene Daten, die auf Endpoints und Servern gespeichert werden, während des gesamten Lebenszyklus.

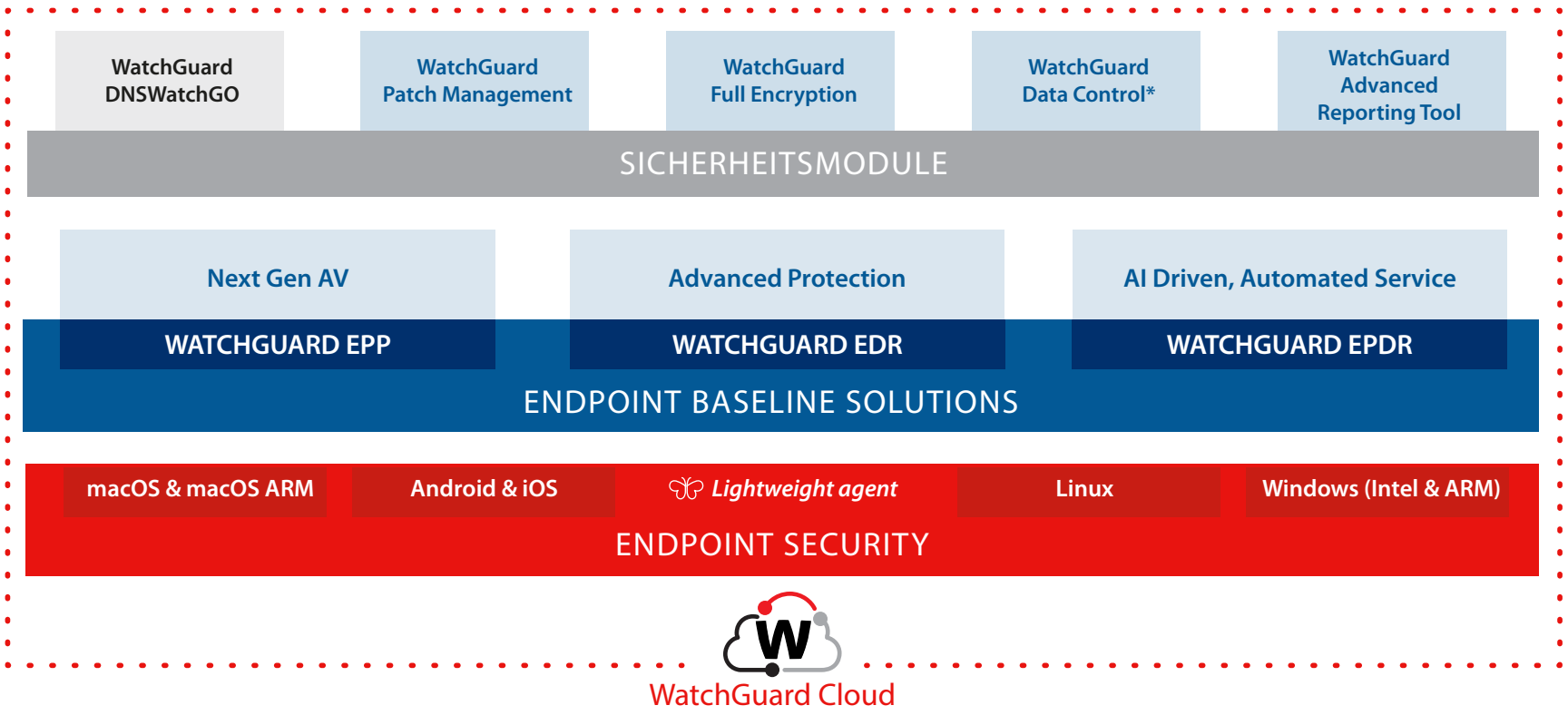
**Data Control ist in den folgenden Ländern verfügbar: Spanien, Deutschland, Vereinigtes Königreich, Schweden, Frankreich, Italien, Portugal, Niederlande, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.*

WatchGuard SIEMFeeder

WatchGuard SIEMFeeder bietet eine neue Quelle für wichtige Details zu den Sicherheitsinformationen aller Prozesse, die auf Ihren Geräten ausgeführt werden, während sie kontinuierlich überwacht werden.

WatchGuard DNSWatchGO

WatchGuard DNSWatchGO bietet Schutz auf DNS-Ebene inklusive Content Filtering, mit dem sich Unternehmen auch jenseits des eigentlichen Netzwerks gegenüber Phishing, Ransomware und anderen Angriffen bestmöglich abschirmen können, ohne dass ein VPN benötigt wird.



Gründe für die Verbesserung Ihrer Sicherheit

1. Fügen Sie Schutz für eine räumlich verteilte Belegschaft hinzu, wenn die Unternehmensrichtlinien für die Arbeit im Homeoffice erweitert werden.

WatchGuard Passport enthält WatchGuard EPDR, WatchGuard DNSWatchGO und WatchGuard AuthPoint für die Multifaktor-Authentifizierung. In Kombination schützen diese Lösungen die Anwender vor den verschiedensten Bedrohungen. Zudem bewahren sie über die Endpoint-Security hinaus die Unternehmensressourcen vor der Infiltration aufgrund verlorener oder gestohlener Zugangsdaten – einer Angriffsmethode, die bei einigen der größten veröffentlichten Sicherheitsverletzungen angewandt wurde.

★ Empfohlene Lösung: **WatchGuard Passport**

2. Wiederherstellung nach einem Angriff oder nach der Erkennung von verborgener Malware auf Endpoints oder in Unternehmensnetzwerken, wenn die Malware von einem Endpoint stammt.

Unternehmen in dieser Position haben zwei Gewissheiten – erstens, dass sie für Cyberkriminelle sicherlich von Interesse sind, und zweitens, dass ihr derzeitiges Schutzniveau nicht angemessen ist. Da sich der erweiterte Schutz von WatchGuard EPDR mit dem Zero Trust Application Service und dem Threat Hunting Service weiterentwickelt hat, ist die Anzahl der auf Malware basierenden Angriffe, die unser Support-Team untersucht/bearbeitet hat, auf nahezu null gesunken – unsere Kunden erleben diese Angriffe also gar nicht mehr. In Kombination mit den Visualisierungs- und Management-Tools zur Steigerung der Produktivität eines überlasteten IT-Teams ist der Service dafür gerüstet, wiederholte Angriffe und teure Behebungsmaßnahmen zu verhindern.

★ Empfohlene Lösung: **WatchGuard EPDR**

3. Fügen Sie als geplante Sicherheitsinvestition die EDR-Funktion zu einer vorhandenen AV-Lösung hinzu.

Diese Unternehmen sind sich der Sicherheitsrisiken am Endpoint bewusst und haben ein AV-Produkt eingeführt. Doch sie wissen, dass sie eine EDR-Lösung benötigen, um Hackern einen Schritt voraus zu sein. Es besteht keine Notwendigkeit, auf eine Verlängerung des AV-Vertrags zu warten. Unsere WatchGuard EDR-Lösung ergänzt eine vorhandene AV-Bereitstellung, so dass Kunden schnell von unserem fortschrittlichen, differenzierten Ansatz profitieren können.

★ Empfohlene Lösung: **WatchGuard EDR**

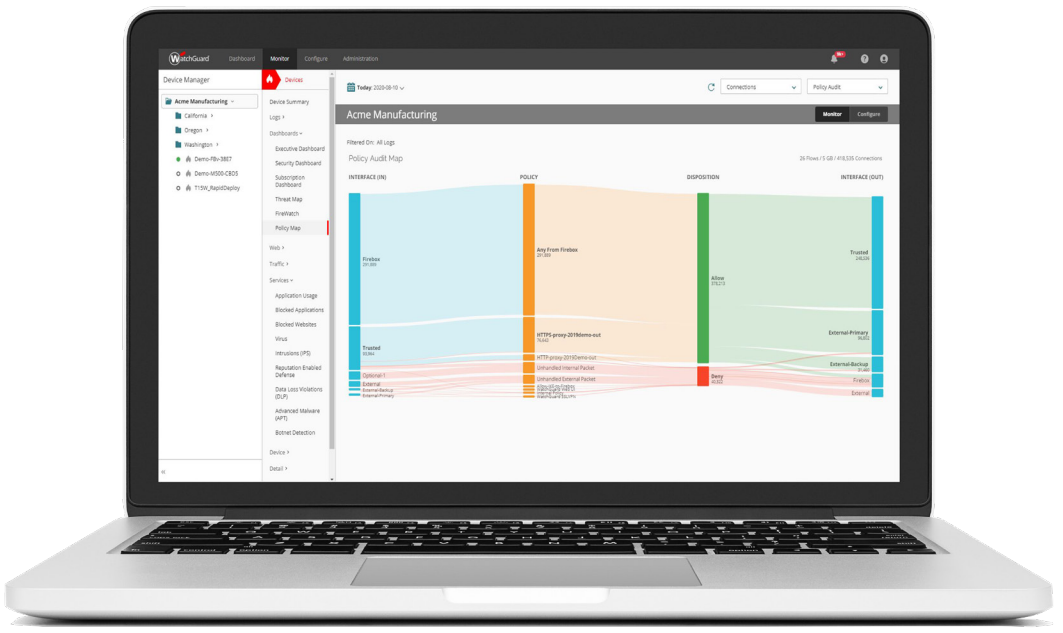
4. Rüsten Sie ausgehend von einem kostenlosen oder auf private Nutzung ausgerichteten Endpoint-AV-Produkt auf.

Manchmal setzen kleinere Unternehmen oder solche, die nur wenige Geräte außerhalb des Netzwerkperimeters haben, auf ein reduziertes Risikoprofil und schieben Investitionen in die Sicherheit auf. Aber die Welt verändert sich. Da Unternehmen immer mehr Risiken ausgesetzt sind und strengere Vorschriften zur Datensicherheit und zum Datenschutz erfüllen müssen, gehen sie zu einer Business-Lösung wie dem Produkt WatchGuard EPP über. WatchGuard EPP ist mit starker signaturbasierter Prävention, einschließlich Signaturen von Malware aus unserer Installationsbasis, sowie Verhaltensanalyse und Filterung von Webinhalten eine kluge Wahl, die zukunftssicher ist, da die Plattform mit dem Geschäftswachstum Schritt hält.

★ Empfohlene Lösung: **WatchGuard EPP**

WatchGuard Cloud

- Erstellung von Verbindungen in Echtzeit, um Aufgaben in Sekundenschnelle auf Tausende von Geräten zu verteilen
- Verwaltung aller Produkte von WatchGuard über eine einzige Konsole
- Anzeigen von Geräten auf mehreren Endpoint-Plattformen, einschließlich Windows, Linux, macOS, iOS und Android



WATCHGUARD-SICHERHEITSPORTFOLIO

Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Smartphones“ als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

Sicheres, cloud-verwaltetes WLAN

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Endpoint-Security

WatchGuard Endpoint-Security ist ein cloud-natives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung WatchGuard EPDR verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Mehr erfahren

Weitere Details erhalten Sie von einem autorisierten WatchGuard-Vertriebspartner oder unter **https://www.watchguard.com/de**.

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für mittelständische und dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im Pazifikraum. Weitere Informationen finden Sie unter **WatchGuard.de**.