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 Advanced 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 Advanced 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-Sicherheit mit WatchGuard EPDR, das alle Vorteile der EDR- und EPP-Produkte von WatchGuard in einem Paket enthält.

WatchGuard Advanced EPDR

- Die zentrale Verwaltung und Suchmaschine für IoCs, die mit STIX- und YARA-Regeln kompatibel ist, ermöglicht Analysten, schnell nach aktuellen Vorfällen zu suchen, Sicherheitsinformationen auszutauschen und die betroffenen Endpoints bei der Vorfallsanalyse zu ermitteln.
- Advanced EPDR entdeckt erweiterte, nicht-deterministische IoAs, die dem MITRE ATT&CK-Framework zugeordnet sind. Die mit diesen IoAs verknüpfte kontextbezogene Telemetrie ermöglicht es Analysten, tiefergehende Untersuchungen durchzuführen.
- Die Remote-Shell ermöglicht weitere Untersuchungen, Eindämmung und Minderung von Bedrohungen. Mit Advanced EPDR können sich Sicherheitsanalysten von der Web-Konsole aus mit den Endpoints des Unternehmens verbinden, um deren Status zu bewerten, einen Vorfall zu untersuchen und Maßnahmen zur Eindämmung eines Angriffs zu ergreifen.

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 unsere EDR-Lösungen 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- und iOS-Geräte.

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.

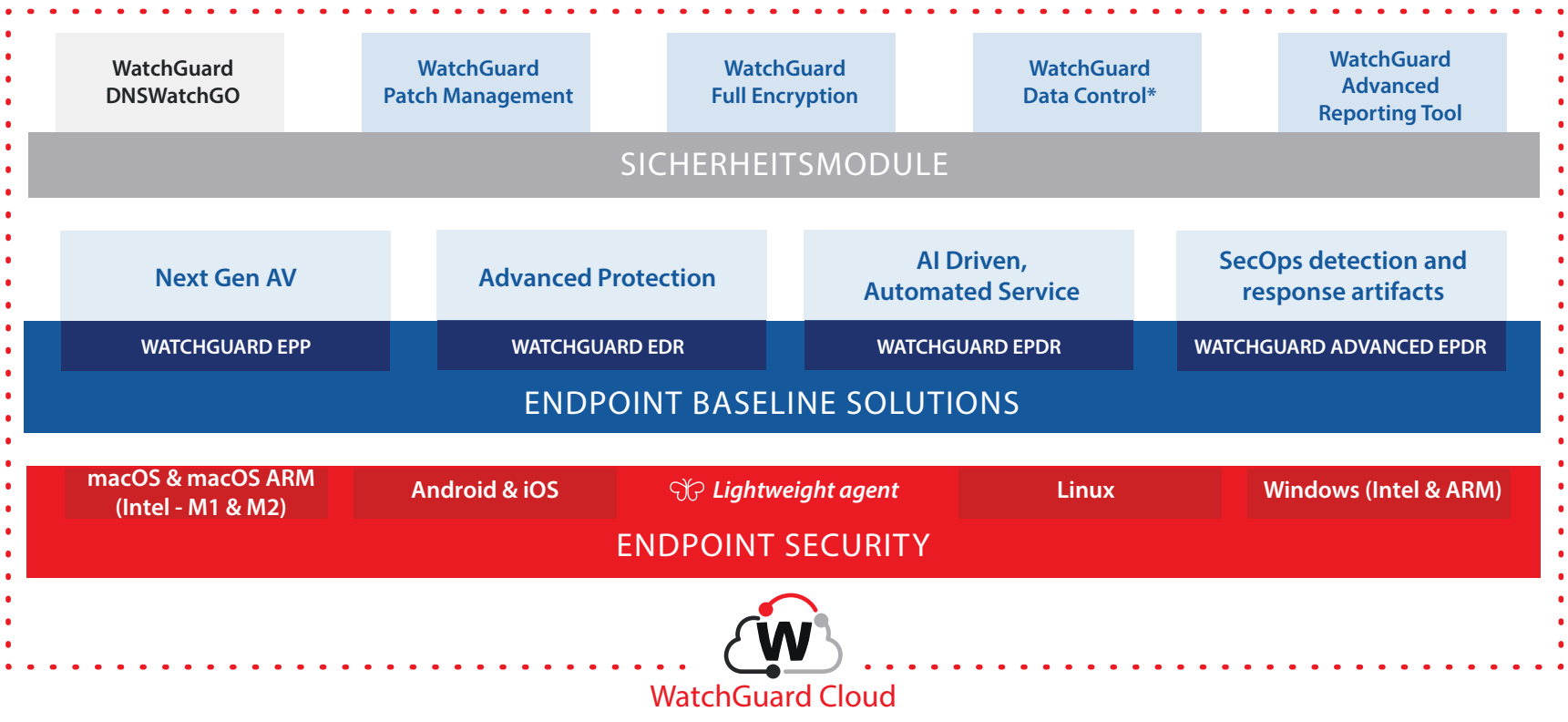
**Data Control ist in den folgenden Ländern verfügbar: Spanien, Deutschland, Vereinigtes Königreich, Schweden, Frankreich, Italien, Portugal, Niederlande, Finnland, Dänemark, Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.*

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.

WatchGuard Advanced EPDR wurde zur Unterstützung von Sicherheitsteams entwickelt und ist das ultimative Tool, um ihre Sicherheitsprozesse zu optimieren. Mit den automatisierten Präventions-, Erkennungs- und Reaktionsfunktionen von WatchGuard EPDR in Kombination mit den zusätzlichen Tools der erweiterten Version sind Sicherheitsteams in Unternehmen der dynamischen und sich ständig weiterentwickelnden Bedrohungslandschaft immer einen Schritt voraus und können von beispiellosem Schutz, Erkennung und Reaktion ohne große Investitionen profitieren.

★ Empfohlene Lösung: **WatchGuard Advanced EDR**

4. 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**

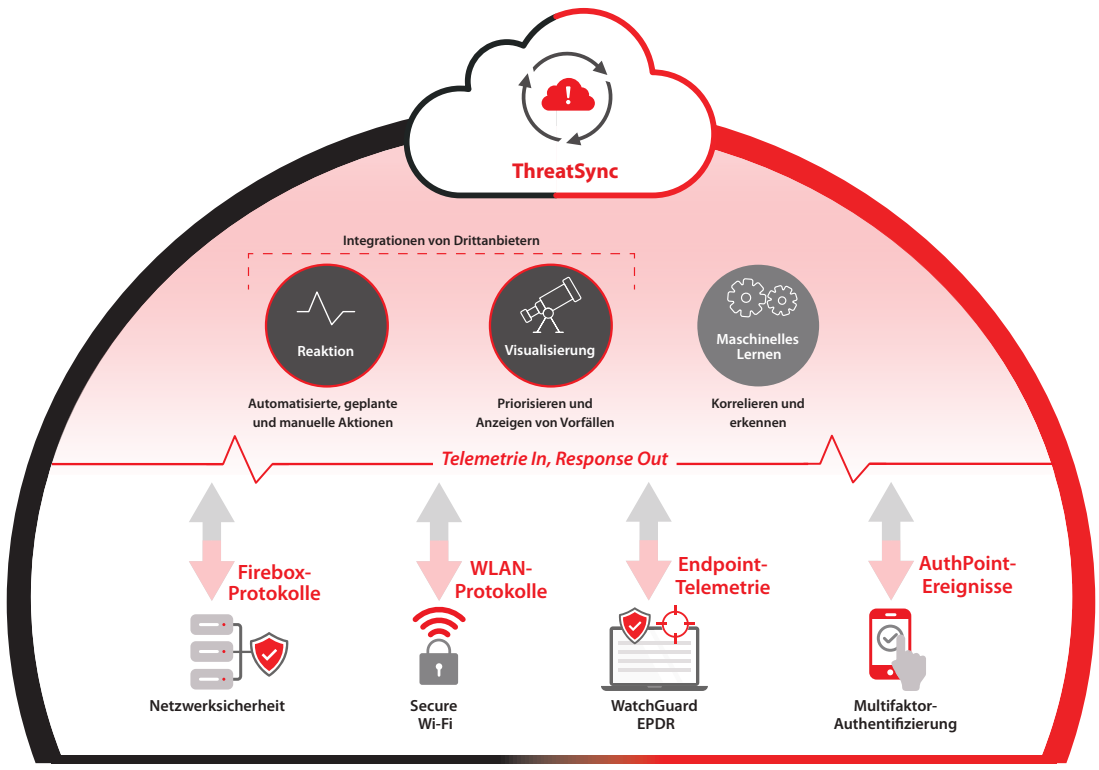
5. Verbessern Sie Ihre Erkennungs- und Reaktionsfähigkeiten, indem Sie auf Advanced EPDR upgraden.

WatchGuard Advanced EPDR wurde zur Unterstützung von Sicherheitsteams entwickelt und ist das ultimative Tool, um ihre Sicherheitsprozesse zu optimieren. Mit den automatisierten Präventions-, Erkennungs- und Reaktionsfunktionen von WatchGuard EPDR in Kombination mit den zusätzlichen Tools der erweiterten Version sind Sicherheitsteams in Unternehmen der dynamischen und sich ständig weiterentwickelnden Bedrohungslandschaft immer einen Schritt voraus und können von beispiellosem Schutz, Erkennung und Reaktion ohne große Investitionen profitieren.

★ Empfohlene Lösung: **WatchGuard EPDR**

Betreten Sie die XDR-Welt und profitieren Sie von umfassender Sicherheit

Mit ThreatSync, Kernkomponente der Unified Security Platform®-Architektur von WatchGuard, bieten wir eine umfassende und einfach zu bedienende XDR-Lösung. Dies ermöglicht es uns, produktübergreifende Erkennungen zu vereinheitlichen und Bedrohungen schneller über eine einzige Schnittstelle zu beheben.



* Secure Wi-Fi und AuthPoint werden in Kürze verfügbar sein und in ThreatSync integriert werden.

DAS WATCHGUARD PORTFOLIO

Netzwerksicherheit

WatchGuard bietet eine breite Palette an Netzwerksicherheitslösungen, von Tabletops und 1-HE-Rackmount-Appliances bis hin zu cloudbasierten und virtuellen Firewalls. Unsere Firebox® Appliances bieten wichtige Sicherheitsdienste, von Standard-IPS, URL-Filterung, Gateway-AV, Anwendungskontrolle und Antispam bis hin zu erweiterten Schutzfunktionen wie Datei-Sandboxing, DNS-Filterung und mehr. Dank der leistungsstarken Deep Packet Inspection (DPI) können Sie alle unsere Sicherheitsdienste gegen Angreifer einsetzen, die versuchen, sich hinter verschlüsselten Kanälen wie HTTPS zu verstecken. Außerdem bietet jede Firebox standardmäßig SD-WAN, was die Ausfallsicherheit und Leistung des Netzwerks erhöht.

Sicheres, cloudverwaltetes WLAN

Die sicheren, cloudverwalteten WLAN-Lösungen von WatchGuard bieten einen sicheren, geschützten Rahmen für WLAN-Umgebungen, ohne dass Sie sich um die Verwaltung kümmern müssen. Gleichzeitig werden die Kosten erheblich gesenkt. Von Heimbüros bis hin zu großflächigen Firmengeländen stellt WatchGuard die WLAN 6-Technologie mit sicherer WPA3-Verschlüsselung bereit. Dank WatchGuard Cloud sind WLAN-Netzwerkkonfiguration und Richtlinienverwaltung, Zero-Touch-Bereitstellung, benutzerdefinierte Captive Portals, VPN-Konfiguration, umfangreiche Interaktionstools, Einblicke in Geschäftsanalysen und Upgrades nur einen Klick entfernt.

Identity Security und MFA

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. AuthPoint bietet ebenfalls eine optimierte Benutzererfahrung mit Online- und Offline-Authentifizierungsmethoden sowie ein Webanwendungsportal für einfachen Single Sign-On-Zugriff.

Endpoint-Sicherheit

Mit den Lösungen von WatchGuard Endpoint Security schützen Sie Ihre Geräte vor Cyber-Angriffen. WatchGuard EPDR und Advanced EPDR, unsere erstklassigen KI-gestützten Endpoint-Lösungen, verbessern Ihre Sicherheitslage durch die nahtlose Integration von Endpoint Protection (EPP) mit Funktionen für Detection and Response (EDR) und unseren Zero-Trust Application und Threat Hunting Services. Diese sind alle vollständig in die WatchGuard Cloud und ThreatSync integriert und bieten wertvolle Einblicke und Erkenntnisse, wobei sie gleichzeitig die produktübergreifende Erkennung und Reaktion (XDR) stützen.

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 Cybersicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres 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 und sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 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 ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com/de.