

Die WatchGuard Unified Security Plattform

Weiterentwicklung Ihrer
MSP-Sicherheitspraxis



ES IST ZEIT FÜR EINEN NEUEN ANSATZ

Die Unified Security Platform von WatchGuard ist speziell darauf ausgelegt, die wachsende Beliebtheit von Managed Security Services sowie selbstverwaltete Bereitstellungen zu unterstützen. Damit wird die moderne Sicherheitsplattform als einheitliche, vereinfachte, leistungsstarke, umfassende, automatisierte, intelligente und transparente Plattform neu definiert, die gezielt auf heutige Servicebereitstellungsmodelle abgestimmt ist.

Unsere Unified Security Platform ersetzt den alten Patchwork-Ansatz für Sicherheit, der zu steigendem Verwaltungsaufwand und vermindertem Schutz vor aktuellen und zukünftigen Bedrohungen geführt hat. Die fünf Elemente der Plattform bilden zusammen die Grundlage für die Verbesserung und Vereinheitlichung der Bereitstellung von Sicherheitsdiensten.

ES IST ZEIT FÜR EINE NEUE VISION

Wir bei WatchGuard sehen eine Zukunft, in der Cybersicherheitstechnologie ebenso leistungsfähig wie anwenderfreundlich ist. Wir wissen, dass wir Ihrem Team eine Technologie zur Verfügung stellen müssen, die für die professionelle Servicebereitstellung optimiert ist, um Ihnen herausragende Sicherheit zu bieten. Diese umfassende Vision gewährleistet, dass Sie die bestmögliche Sicherheit erhalten, unabhängig davon, wie Sie diese einsetzen möchten.

ES IST ZEIT FÜR WATCHGUARD

Sie haben die Möglichkeit, ein beträchtliches Wachstumspotenzial zu erschließen, und zwar mit einem Sicherheitsportfolio, das problemlos skalierbar und der anspruchsvollen Bedrohungslage von morgen gewachsen ist. Um von dieser Chance zu profitieren, müssen Sie sich für den richtigen Technologiepartner entscheiden, der Cybersicherheitsdienste aus einer Hand anbietet und eine Plattform bereitstellt, welche die Effizienz und Bereitstellung von Sicherheitsservices verbessert. Wir bei WatchGuard gehen die Dinge anders an und wir haben unsere Unified Security Platform so konzipiert, dass sie Ihnen jetzt und in Zukunft die besten Dienste leistet.

„Entkoppelte Sicherheitslösungen sind nicht nur schwer zu verwalten. Sie machen auch eine Erkennung von Bedrohungen und Schwachstellen fast unmöglich. Mit der Unified Security Platform™ von WatchGuard können Unternehmen ihre Sicherheitsmechanismen verbessern und erweitern. Gleichzeitig kann der betriebliche Aufwand reduziert und mit anwenderorientierten Sicherheitsansätzen die Risikominderung vereinfacht werden.“

~ Tom Ruffolo



VEREINFACHUNG DURCH ZENTRALISIERUNG

Cybersicherheit kann komplex sein und die erforderlichen Technologien, um mit Cyberkriminellen Schritt zu halten, werden immer anspruchsvoller. Durch die Zentralisierung der Sicherheitsfunktionen werden all diese Technologien in einer Plattform vereint, die Unternehmen ohne eigene Sicherheitsteams auf einfache Weise nutzen können. Es geht darum, Werkzeuge und Ressourcen bereitzustellen, die das Sicherheitsmanagement vereinfachen und Unternehmen zugleich das benötigte Sicherheitsniveau bieten – nicht nur heute, sondern auch in Zukunft.

WatchGuard hat sich dieser Mission verschrieben. Wir möchten die Bereitstellung des intelligentesten Sicherheitsportfolios so einfach wie irgend möglich machen.

Dies steht bei allem, was wir tun, im Mittelpunkt.

Das Fehlen einer einheitlichen Strategie für Cybersicherheit ist der Hauptgrund dafür, warum Unternehmen Opfer eines Ransomware-Angriffs werden.

~ Unterstützt von Pulse



DIE WATCHGUARD UNIFIED SECURITY PLATFORM

Das heutige Wirtschaftsumfeld ist auf den Internetzugang über verschiedene IT-Umgebungen und Standorte hinweg angewiesen. Dabei stellt jede ihre eigenen Anforderungen an die Cybersicherheit. Ob Sie physische oder virtuelle Infrastrukturen, Anwender, Netzwerke, Endpunkte oder WLAN-Umgebungen an einem oder mehreren Standorten schützen müssen: Die Unified Security Platform erlaubt Ihnen ein wirksames, unternehmensweites Sicherheitsmanagement.

95 % der MSPs sind der Auffassung, dass der Wechsel zwischen mehreren Verwaltungsoberflächen, um die Sicherheit für einen einzelnen Kunden zu verwalten, beim Team zu Produktivitätseinbußen führt.

~ Unterstützt von Pulse

UMFASSENDE SICHERHEIT

Das umfassende Portfolio von WatchGuard unterbricht die Cyber Kill Chain in jeder einzelnen Phase. Schieben Sie unbefugtem Datenzugriff, der Ausbeutung anfälliger Systeme, Phishing, Ransomware, Eindringversuchen und ausgereifter Malware für alle Ihre Anwender, Umgebungen und Geräte einen Riegel vor.

BETRIEBLICHE AUSRICHTUNG

WatchGuard bietet ein optimales Sicherheitskonzept für Ihr Unternehmen mit drei wichtige Kaufoptionen für Partner, darunter Vorauszahlung mit fester Laufzeit, Pay-as-You-Go mit fester Laufzeit und Pay-as-you-go ohne Laufzeit. Integrieren Sie WatchGuard problemlos in Ihr Ökosystem mit plattformübergreifenden RESTful-APIs.

TRANSPARENZ UND KONTROLLE

WatchGuard Cloud ist die zentrale Managementschnittstelle mit Visualisierungs- und Reporting-Tools für die gesamte Unified Security Platform, über die technische Teams die gesamte WatchGuard-Sicherheitsstruktur von einem Punkt aus umfassend verwalten können.

KOLLEKTIVE INTELLIGENZ

Ganz gleich, wie fortschrittlich die Technologie ist: Wenn Sicherheitsschichten unabhängig voneinander bereitgestellt werden, ist die Gefahr groß, dass ein Angreifer ein Schlupfloch in diesem Gerüst findet. Mithilfe von Korrelation und einem starken, über eine einzige Plattform bereitgestellten Identitätsframework können Sie Lücken bei der Transparenz schließen und Schwachstellen bei der Sicherheit ausleuchten.

AUTOMATISIERUNG

Automatisierung steht im Mittelpunkt von WatchGuards Unified Security Platform. Sie trägt zur Beschleunigung von Prozessen, zur Bekämpfung von Bedrohungen und zu einer effizienteren Arbeitsweise von IT-Teams bei. Der Automation Core von WatchGuard generiert eine interaktionsfreie sicherheitsbezogene Feedbackschleife und beschleunigt das geschäftsorientierte Sicherheitsmanagement.





UMFASSENDE SICHERHEIT

In einer Welt, in der sich die Cybersicherheitslandschaft ständig verändert und jeden Tag neue Bedrohungen aufkommen, macht WatchGuard Cybersicherheitstechnologie auf Enterprise-Niveau für jedes Unternehmen erschwinglich. Ein wirksamer Schutz vor den unzähligen heutigen Bedrohungen erfordert ein intelligentes Zusammenspiel unterschiedlicher Dienste. Durch branchenführende Netzwerk- und Endpunktsicherheit, sicheres WLAN, Multifaktor-Authentifizierung sowie Produkte und Services im Bereich der Network Intelligence ermöglicht WatchGuard über 250.000 Unternehmen weltweit den Schutz ihrer wichtigsten Ressourcen.



Netzwerksicherheit

WatchGuard bietet eine große Palette an Network Security-Lösungen, von Tabletops und 1-HE-Rackmount-Appliances bis hin zu cloudbasierten und virtuellen Firewalls. Die Firebox unterstützt eine Vielzahl wichtiger Sicherheitsdienste, darunter Standard-IPS, URL-Filterung, Gateway-AV, Anwendungskontrolle und Spamschutz, sowie Dienste zur Bekämpfung fortgeschrittener Bedrohungen wie Datei-Sandboxing, DNS-Filterung und mehr. Leistungsfähige Deep Packet Inspection (DPI) bedeutet, dass die gesamte Bandbreite der WatchGuard-Dienste genutzt werden kann, um Angriffe abzuwehren, die sich in verschlüsselten Kanälen wie HTTPS verbergen. Außerdem bietet jede Firebox standardmäßig SD-WAN, was die Ausfallsicherheit und Leistung des Netzwerks erhöht.

Multifaktor-Authentifizierung

Der AuthPoint-Dienst von WatchGuard ist die richtige Lösung zur rechten Zeit, um auf einer benutzerfreundlichen Cloud-Plattform effektive Authentifizierung bereitzustellen. MFA ist der sicherste Ansatz der Benutzeridentifizierung. Nach der Eingabe der Anmeldedaten auf einem Gerät wird der Identitätsnachweis über ein weiteres Gerät als zusätzlichen Faktor vorausgesetzt. Die mobile AuthPoint-App sorgt dank einfacher Push-Benachrichtigungen für eine umfassende Transparenz der Anmeldeversuche, sodass Benutzer den Zugriff direkt über ihr Smartphone gewähren oder blockieren können.

Sicheres WLAN

Die sichere WLAN-Lösung 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 umfasst eine Reihe erweiterbarer Lösungen, um Sicherheitsverletzungen, Datendiebstahl und Cyberangriffe zu vermeiden. In unserer cloudbasierten Plattform sind die Technologie, die Intelligenz und das Fachwissen integriert, um fortschrittliche Funktionen für Prävention, Erkennung, Eindämmung und Reaktion über einen ressourcensparenden Agenten bereitzustellen. Wenn Sie Produkte wie DNSWatchGO für den Schutz von Endpunkten auf DNS-Ebene in dasselbe Angebot aufnehmen, erhalten Sie Schutz für den gesamten Lebenszyklus von Bedrohungen.



Verlassen Sie sich nicht nur auf das, was wir sagen. [Bewertungen von Trust Radius >](#)





TRANSPARENZ UND KONTROLLE

WatchGuard Cloud ist die zentrale Verwaltungsschnittstelle mit Visualisierungstools für die gesamte Unified Security Platform. Als zentrale Instanz für die Verwaltung, Verteilung und Durchsetzung von Sicherheitsrichtlinien in Ihrem Unternehmen ermöglicht Ihnen WatchGuard Cloud die nahtlose Verwaltung der gesamten WatchGuard-Implementierung und die Erstellung entsprechender Berichte, ohne dass Sie sich bei unterschiedlichen Systemen anmelden müssen.

91 % der MSPs sind der Überzeugung, dass cloudbasierte Lösungen und eine zentrale Benutzeroberfläche Voraussetzungen sind um effizient arbeiten zu können.

~ Pulse

Sicherheit, die Sie sehen können

Mittels WatchGuard Cloud können Sie auf einfache Weise umsetzbare Sicherheitstrends erkennen, die Effizienz von Sicherheitsdiensten überwachen und schnell Geschäfts-, Compliance- und Sicherheitsberichte mit beeindruckenden Visualisierungstools erstellen. Zeigen Sie wichtige Anwenderinformationen an, um Sicherheitsmuster zu verstehen und potenzielle Risiken zu erkennen. Wählen Sie aus über 100 umfangreichen Berichten und Dashboards aus. Zudem gibt es die Möglichkeit, Berichte nach Plan zu erstellen und per E-Mail an wichtige Beteiligte zu senden, von der Geschäftsleitung und IT-Leitern über Netzwerkverantwortliche und Sicherheitsanalysten bis hin zu HR-Managern und Abteilungsleitern.

Universelle Richtlinienverwaltung

WatchGuard Cloud wurde mit Blick auf die betriebliche Effizienz konzipiert: Richtlinienerstellung und -verteilung werden damit zu einem Kinderspiel. Erstellen Sie Richtlinienvorlagen für eine einfache und wiederholbare Bereitstellung über viele Clients. Konfigurieren Sie Authentifizierungsrichtlinien, um anzugeben, bei welchen Ressourcen sich Anwender authentifizieren können und welche Authentifizierungsmethoden sie verwenden müssen. Erstellen Sie in Sekundenschnelle Endpunktsicherheitsrichtlinien für Tausende von Computern und wenden Sie diese an. Außerdem können Sie mithilfe von WatchGuard Cloud Reaktionsmaßnahmen automatisieren, Warnungen minimieren und die Eindämmung infizierter Geräte unterstützen.

Umgehend verwertbare Sicherheitsinformationen

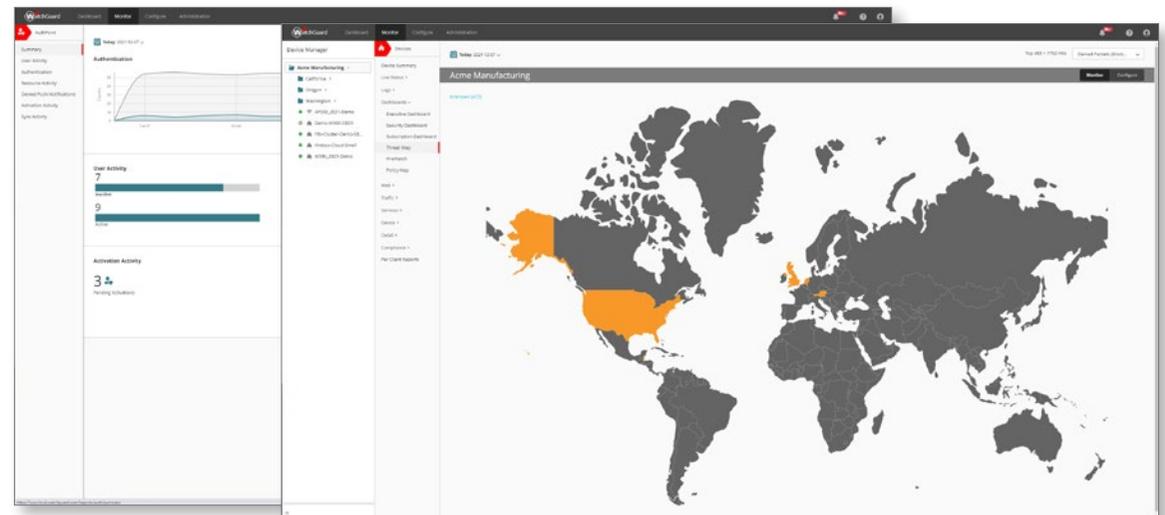
Wenn Sie nicht sehen können, was in jedem Winkel Ihrer IT-Infrastruktur vor sich geht, dürfen Sie das nicht auf die leichte Schulter nehmen. Diese toten Winkel stellen ein massives Sicherheitsrisiko dar. WatchGuard ermöglicht Ihnen eine umfassende Visualisierung Ihres gesamten Netzwerks. Dies erreichen wir, indem wir Visualisierungsdienste der Spitzenklasse in jedes einzelne Produkt integrieren. Wir geben Ihnen über 100 Dashboards und Berichte an die Hand, mit denen Sie den Überblick behalten und Informationen bis auf Protokolldatenebene aufschlüsseln können.

Effektive Echtzeitüberwachung

Entschärfen Sie Risiken durch die proaktive Überwachung potenzieller Sicherheitsschwachstellen oder Probleme in Bezug auf die Netzwerkeffizienz, und gewährleisten Sie gleichzeitig die Effektivität der Sicherheitsrichtlinien. Anhand zahlreicher interaktiver visueller Dashboards, auf denen Daten in Echtzeit übersichtlich dargestellt werden, können Sie Problembereiche schnell identifizieren und haben die Möglichkeit, Daten zu filtern und auszuwerten, um zusätzliche Details zu erhalten. Sie können sich einen Überblick über den Netzwerkverkehr verschaffen, sehen, welche Anwendungen die größte Bandbreite beanspruchen und weitaus mehr.

Erstellung umfassender Berichte

Sie haben Zugriff auf ein breites Spektrum an Berichten, die Sie sowohl zusammenfassend als auch im Detail über Richtlinienutzung, Compliance, Netzwerk- und Datenverkehr, Sicherheitsdienste, Dialog-, Benutzeranalysen und Gerätetstatistiken informieren. Berichte sind jederzeit abrufbar und können im Rahmen vorbeugender und korrekiver Maßnahmen automatisch zugestellt werden.





KOLLEKTIVE INTELLIGENZ

Die Funktionen zum Informationsaustausch der WatchGuard Unified Security Platform verbessern den Schutz vor gezielten Bedrohungen, verkürzen die Zeit bis zur Erkennung von Monaten auf Minuten und reduzieren die Bedrohung durch Zero-Day-Angriffe und getarnte Malware.

Nur 19 % der MSPs erwarten, dass eine zentrale Sicherheitsplattform Sicherheitserkenntnisse produktübergreifend nutzen und die Reaktion auf Vorfälle automatisieren kann.

~ Pulse

Die Kraft der Korrelation

Als integrierte Plattform für erweiterte Erkennung und Reaktion (Extended Detection and Response, XDR) über Umgebungen, Anwender und Geräte hinweg überwacht ThreatSync die gesamte Unified Security Platform, sodass Sie die Bösewichte auf frischer Tat ertappen und sie aufhalten können. Durch die Nutzung der Cloud zur gemeinsamen Verwendung von Telemetriedaten werden Endgeräte über Angriffe auf das Netzwerk informiert. Angriffe auf Endgeräte werden zudem sogar beim Roaming transparent.

ThreatSync korreliert automatisch Indikatoren in Ihrer gesamten Sicherheitsstruktur und vergibt eine eindeutige Bedrohungsbewertung, um einen Alarm auszulösen. Durch die Verknüpfung von Telemetriedaten über Netzwerk, Benutzer, Endpunkte und Anwendungen hinweg werden verborgene Bedrohungen aufgedeckt, sodass Sie schneller reagieren können. Wird eine Bedrohung identifiziert, tritt ThreatSync sofort in Aktion. Der infizierte Endpunkt wird isoliert, die Malware wird bis zur Behebung des Problems blockiert und ein Übergreifen auf andere Teile Ihres Netzwerks wird verhindert.

Identity Framework

Mit dem Identity Framework führt die Unified Security Platform verifizierte Identität als Element in jede Sicherheitsanalyse ein und verbessert das Identitätsmanagement mit flexiblen Regeln zur risikobasierten Konfiguration von Anwendern und Geräten. Mit dem Identity Framework können Sie Zugriff auf der Grundlage der Rollen- oder Gruppenzuweisungen eines Anwenders gewähren. Ist der Anwender zum Beispiel im Marketing, im Vertrieb, in der Technik oder im Finanzbereich tätig? Ist er ein Mitarbeiter, Partner oder Kunde?

Ideal für Zero-Trust-Netzwerke

Bei Netzwerkansätzen nach dem Prinzip Zero-Trust werden Endpunkttelemetrie und Anwenderrisiken berücksichtigt, bevor über VPN Zugriff auf das Netzwerk gewährt wird. Dadurch wird verhindert, dass durch einen angegriffenen Endpunkt Malware und Eindringlinge in die restliche Umgebung eindringen können. Dieses Sicherheitsprinzip des „Vertraue niemandem, verifiziere jeden“ ist besonders effektiv für verteilte Sicherheitsteams. In der Unified Security Platform umfassen Zero-Trust-Richtlinien die Verifizierung von Geräten, Anwendungen und Identitäten und die entsprechende Umsetzung. Dies ermöglicht Unternehmen, anhand einer Mikro-Segmentierung die Gefahr von internen Bedrohungen, Netzwerkinfiltration und lateralen Bewegungen im gesamten Netzwerk zu minimieren.





BETRIEBLICHE AUSRICHTUNG

Die WatchGuard Unified Security Platform ist ein wahres Kraftpaket für IT-Teams. Durch die bedienerfreundliche Integration von WatchGuard Firebox-Appliances mit den Lösungen für Authentifizierung, Endpoint-Sicherheit und WLAN wird ein umfassendes, mehrschichtiges Sicherheitskonzept umgesetzt. Unabhängig davon, wie die Serviceverträge mit Ihren Kunden gestaltet sind, ob Sie sie im Voraus oder regelmäßig abrechnen, bieten wir Flexibilität beim Kauf von Produkten und Services über WatchGuard FlexPay. Das stellt eine Lösung sicher, die bestmöglich auf Ihr Geschäftsmodell abgestimmt ist. WatchGuard FlexPay beinhaltet Vorabbezahlung mit fester Laufzeit, Pay-as-you-Go mit fester Laufzeit und Pay-as-you-Go ohne Verpflichtungen.

96 % der MSPs sind derzeit dabei, Anbieter zu konsolidieren oder planen, damit im Jahr 2022 zu beginnen.

~ Pulse

PSAs und RMMs

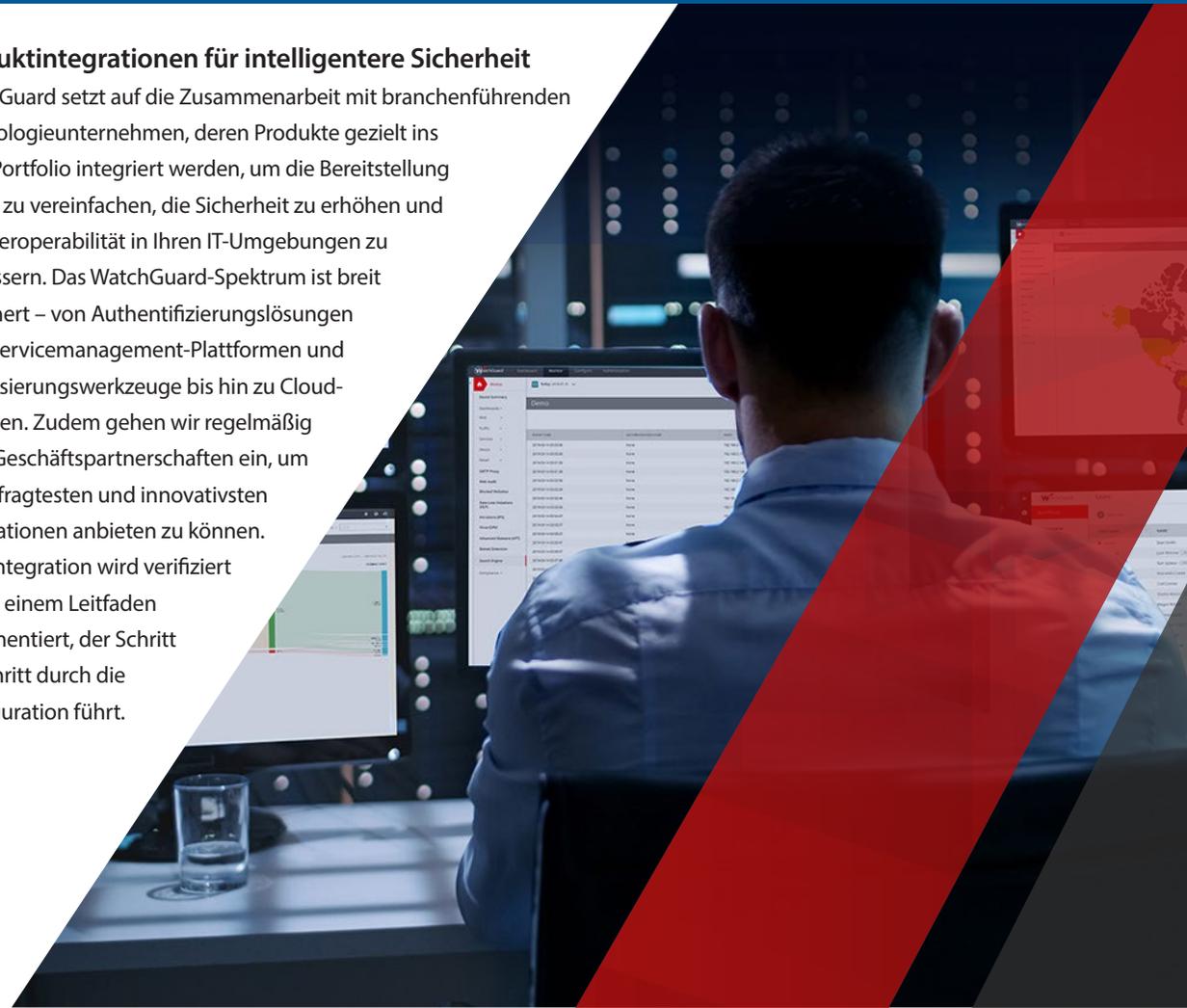
Wir haben uns mit den führenden Anbietern im Bereich PSA (Professional Service Automation) und RMM (Remote Monitoring Management) zusammengetan, um sofort einsatzbereite Integrationen anzubieten, die in wenigen Minuten konfiguriert werden können. Diese Integrationen umfassen die Automatisierung von Service-Tickets, die Synchronisierung von Asset-Informationen zwischen Plattformen, automatisierte Berichte, die von WatchGuard-Daten abgeleitet sind, sowie die Möglichkeit, Konfigurationsänderungen zu übertragen und Sicherheitsereignisse mithilfe von SNMP- und Syslog-Standardprotokollen zu überwachen.

Interoperabilität für Ihre sämtlichen Anwendungen

Außerdem entwickeln wir ständig enge Integrationen mit führenden Cloud-Anwendungen, Security Information Event Management (SIEM), Authentifizierungsanbietern, Cloud Access Security Brokers (CASB), Schwachstellenbewertungen, SD-WAN-Diensten, VoIP-Anbietern und vielem mehr. Diese Integrationen erhöhen die Interoperabilität in Ihrem IT-Stack und in den Umgebungen Ihrer Kunden, steigern die Sicherheit, vereinfachen die Bereitstellung und optimieren die laufende Verwaltung der Anwendungen. Erstellen Sie ein Portfolio-Angebot, das mehrere IT-Kategorien umfasst, und stellen Sie es dann als ein eng integriertes Managed-Service-Angebot bereit.

Produktintegrationen für intelligentere Sicherheit

WatchGuard setzt auf die Zusammenarbeit mit branchenführenden Technologieunternehmen, deren Produkte gezielt ins UTM-Portfolio integriert werden, um die Bereitstellung weiter zu vereinfachen, die Sicherheit zu erhöhen und die Interoperabilität in Ihren IT-Umgebungen zu verbessern. Das WatchGuard-Spektrum ist breit gefächert – von Authentifizierungslösungen über Servicemanagement-Plattformen und Visualisierungswerkzeuge bis hin zu Cloud-Diensten. Zudem gehen wir regelmäßig neue Geschäftspartnerschaften ein, um die gefragtesten und innovativsten Integrationen anbieten zu können. Jede Integration wird verifiziert und in einem Leitfaden dokumentiert, der Schritt für Schritt durch die Konfiguration führt.



UMFASSENDE AUTOMATISIERUNG



Der einzigartige Automation Core von WatchGuard generiert eine interaktionsfreie sicherheitsbezogene Feedbackschleife und beschleunigt das geschäftsorientierte Sicherheitsmanagement. Mit dem Automation Core können Sie die Sicherheitsfunktionen nahtlos auf jede Computerumgebung Ihres Unternehmens ausweiten. Er definiert einen intelligenten, eigenständigen Perimeter, der sich vom LAN über die Cloud bis zum Endpunkt erstreckt. Somit profitiert Ihr Unternehmen von einem kontinuierlichen, integrierten Schutz. Der Automation Core gewährleistet einen sicheren Anwenderzugriff auf wichtige Ressourcen, wehrt hoch entwickelte Bedrohungen vor dem Eindringen in Ihr Netzwerk ab, schützt Endpunkte vor Malware und optimiert die Netzwerkleistung. Zudem erfordert er nur minimale Interaktion seitens Ihres IT-Teams.

*Ein mittelständisches Unternehmen benötigt etwa 800 Tage, um eine Sicherheitsverletzung aufzudecken.
~ Verizon Data Breach Report*

Wirksamkeit der Sicherheitsmaßnahmen

- Im vergangenen Jahr hat jede Firebox durchschnittlich etwa 2.000 Malware-Dateien blockiert, von denen fast 70 % im verschlüsselten Internet-Datenverkehr versteckt waren. Zudem hat jedes Gerät durchschnittlich 300 weitere Netzwerkangriffe abgewehrt.
- Die leistungsstarke HTTPS-Prüfung der Firebox deckt Malware auf, die sich im verschlüsselten Datenverkehr versteckt und in der Regel über 50 % aller potenziellen Malware-Bedrohungen für ein Unternehmen ausmacht.
- Bei den aktuellen Tests von NSS Labs erwies sich WatchGuard als eine von nur zwei Firewall-Plattformen, denen KEINE verborgene Malware entgangen war. WatchGuard hat in drei aufeinanderfolgenden Jahren die Bewertung „Recommended“ (Empfohlen) erhalten.
- Unser Zero-Trust Application Service klassifiziert automatisch ausführbare Dateien. Dazu werden verdächtige Prozesse und Anwendungen mithilfe von proprietären Algorithmen des maschinellen Lernens analysiert, um zwischen Malware und vertrauenswürdigen zu unterscheiden.

Erweiterbarkeit

- Schützen Sie Ihre Anwender innerhalb und außerhalb des Netzwerks vor Phishing, Malware und Ransomware.
- Isolieren Sie Endpunkte und bekämpfen Sie Bedrohungen weltweit.
- Steuern Sie den Zugriff auf Ressourcen, Konten und Informationen mit integrierter Multifaktor-Authentifizierung und mit Single-Sign-On-Bereitstellungen (SSO) für einen zentralen Zugang zu Anwendungen in der Cloud sowie auf interne Ressourcen über RDP und SSH.
- Wenden Sie detaillierte Richtlinien nahtlos auf Anwender und Geräte an, die sich im Netzwerk an- oder abmelden.
- Erkennen, klassifizieren, prüfen und überwachen Sie unstrukturierte personenbezogene Daten, die auf Endpunkten und Servern gespeichert werden, mit Data Control.

Stärkere Auslastung des IT-Personals

- Mit leistungsfähigen plattformübergreifenden Sichtbarkeitstools sparen Sie Hunderte von Stunden bei der Suche nach zeitkritischen Antworten zu Nutzung und Anomalien.
- Reduzieren Sie den Zeit- und Kostenaufwand für die Einrichtung und Konfiguration von Firewall-Geräten um 99 %.
- Erkennen, klassifizieren, prüfen und überwachen Sie unstrukturierte personenbezogene Daten, die auf Endpunkten und Servern gespeichert werden, mit Data Control.
- Mit Patch Management können Sie Updates und Patches für Betriebssysteme, Drittanbieteranwendungen und nicht unterstützte Software-Programme (EOL) zentral verwalten.
- Führen Sie MFA für Ihr Unternehmen ein und nutzen Sie die schnelle, von Assistenten geführte Bereitstellung, die den Konfigurationsaufwand für Sie vereinfacht.
- Mit dem Dark Web Scan-Tool bleiben Sie auf dem Laufenden über kompromittierte E-Mail-Konten, die bei Datenschutzverletzungen in Umlauf gebracht wurden.



Eine profitable Plattform für jedes Bereitstellungsmodell

Mit der Unified Security Platform können Sie Zeit, Geld und Nerven bei der Sicherheitsbereitstellung sparen, ganz gleich, ob Ihr Unternehmen umfassende IT-Dienstleistungen anbietet, spezielle Herausforderungen löst oder Produkte und Dienstleistungen weiterverkauft. Die Unified Security Platform wurde entwickelt, um MSPs bei der Verbesserung und Erweiterung ihres Sicherheitsangebots zu unterstützen.

1 Vertrieb und Onboarding von Kunden

- Sicherheit als Add-on oder Upselling durch sofortige Integrationen mit branchenführenden Technologieplattformen
- Mit einer mehrschichtigen, mandantenfähigen Architektur können Sie beliebig viele Kunden aufnehmen.
- Gewährleisten Sie die Trennung von Daten zwischen Mandanten.

2 Bereitstellung

- Vorab konfigurieren und über die Cloud bereitstellen – es müssen keine Mitarbeiter vor Ort sein!
- Einfache Verwaltung von Software- und Gerätelizenzen
- Vorlagen machen es denkbar einfach, die Bereitstellung beim ersten Mal korrekt durchzuführen!

3 Laufende Verwaltung

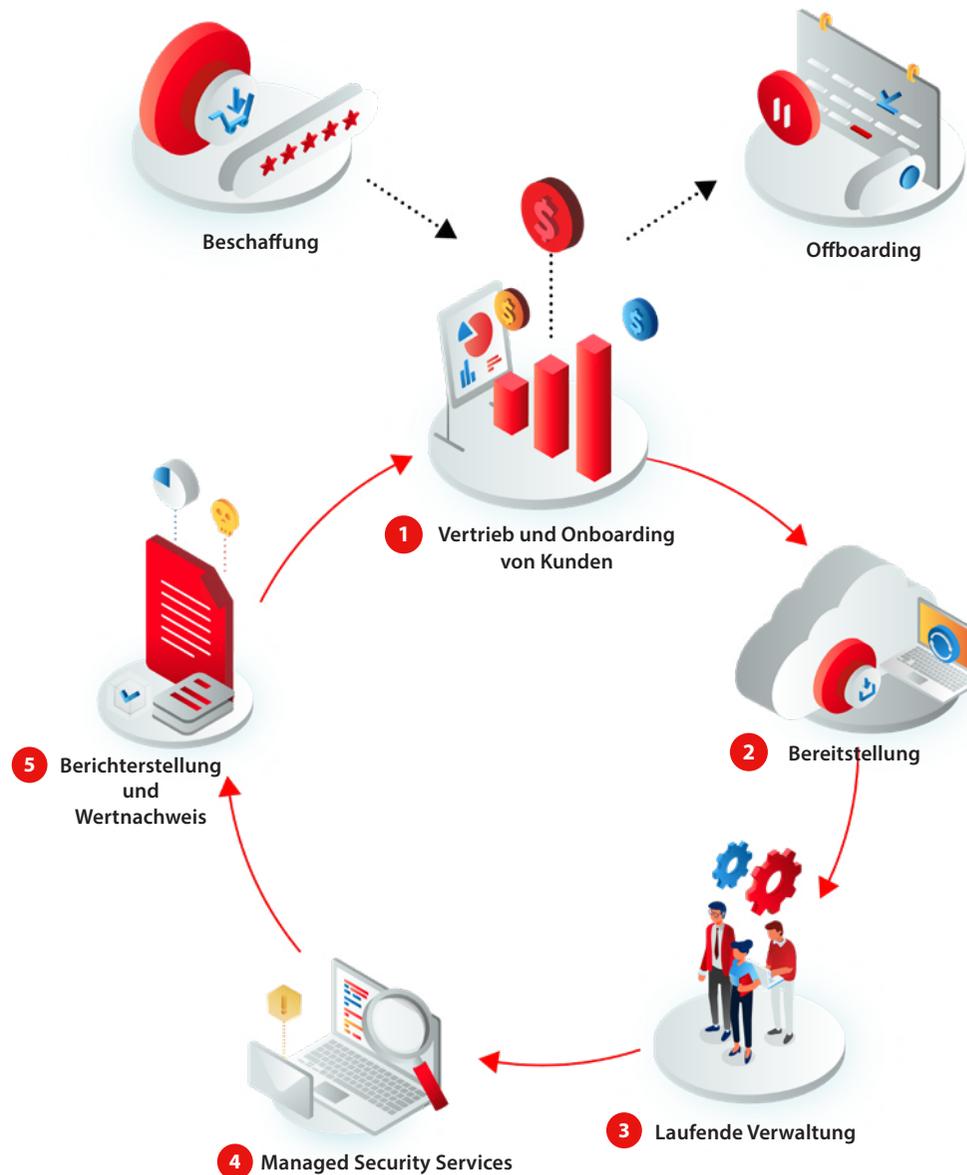
- Unterstützen Sie Ihr Team mit einer zentralen Verwaltung.
- Schaffen Sie manuelle Aufgaben mit dem Automation Core ab.
- Alternativ können Sie den WatchGuard-Stack mit den RMM- und PSA-Tools verwalten, die Sie bereits verwenden.

4 Managed Security Services

- ThreatSync macht es einfach, End-to-End-MDR mit automatischer Telemetrie-Korrelation, Bedrohungsbewertung und Reaktionen im gesamten Stack anzubieten.

5 Berichterstellung und Wertnachweis

- Das Senden fest terminierter oder ad hoc erstellter Berichte an wichtige Kunden-Stakeholder für Quartalsprüfungen lässt sich problemlos konfigurieren. Dabei können sich die Themen auf Bedrohungstrends, Gefährdung durch das Dark Web, Bandbreitennutzung, Compliance-Status und vieles mehr erstrecken.



Beschaffung

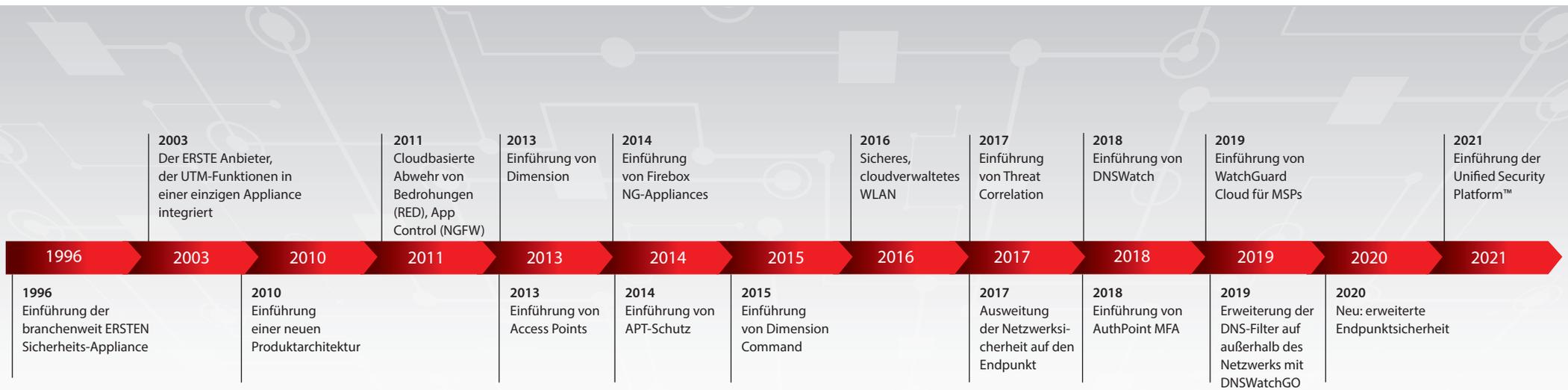
Gemäß unserem MSP-Punktesystem können Sie Punkte vorab erwerben und diese nach Bedarf auf WatchGuard-Lösungen anwenden. Sie können sogar mehrere Käufe gleichzeitig durchführen, um den besten Preis zu erzielen.

Offboarding

Es ist nie schön, einen Kunden zu verlieren, aber mit WatchGuard können Sie Sicherheitsdienste schnell aktivieren oder deaktivieren, um den sich ändernden Kundenanforderungen gerecht zu werden. Mit der monatlichen Option können Sie bei Bedarf sogar jederzeit pausieren oder kündigen und geleaste Hardware an WatchGuard zurückgeben.

Seit 25 Jahren Wegbereiter in puncto Cybersicherheit

WatchGuard ist seit 25 Jahren Wegbereiter bei der Entwicklung innovativer Cybersicherheitstechnologie und stellt sie in einer anwender- und verwaltungsfreundlichen Lösung bereit. Durch branchenführende Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung, erweiterte Endpunktsicherheit sowie Produkte und Dienstleistungen im Bereich der Network Intelligence ermöglicht WatchGuard über 250.000 Kunden weltweit den Schutz ihrer wichtigsten Ressourcen – in einer Welt, in der die Zahl neuer Bedrohungen in der Cybersicherheitslandschaft tagtäglich wächst.



1996
gegründet



Firmensitz: Seattle
im US-Bundesstaat
Washington



7 Betriebszentren und
Direktvertretungen in
21 Ländern



1.200 Mitarbeiter



Über
250.000 Kunden



Über
100 Distributoren



Über 16.000 aktive
Vertriebspartner

Erfolg auf Enterprise-Niveau

WatchGuard ist nachweislich in der Lage, die Konkurrenz durch neue Sicherheitsdienste zu übertreffen und so den Mehrwert für Endkunden und Partner zu erhöhen. WatchGuard sorgt dafür, dass seine Partner und Kunden schnellstmöglich Zugang zu den Produkten und Diensten erhalten, die sie am dringendsten benötigen – ganz gleich, ob es sich um die Markteinführung einer völlig neuen Lösung wie AuthPoint, die Übernahme einer führenden Lösung wie Endpoint Security, das Hinzufügen eines weiteren Sicherheitstools (z. B. APT Blocker für Sandboxing) zu einer bestehenden Lösung oder das Upgraden eines bestehenden Dienstes wie Gateway Antivirus handelt.



100 Prozent Channel, jederzeit

Nicht alle Channel-Programme sind gleich. Sie benötigen eine Partnerschaft, die flexibel genug ist, um sich an Ihr einzigartiges Geschäftsmodell und Ihre Markteinführungsstrategie anzupassen. Sie benötigen eine Partnerschaft, die einfach zu verstehen ist und unkompliziert Vorteile bietet. Sie benötigen eine Partnerschaft, die Ihr Unternehmen wirklich wertschätzt.

Wir bieten Ihnen ein einzigartiges Channel-Programm.

Jeder Geschäftsabschluss, jedes verkaufte Produkt und jeder neue Kunde ist ein Gewinn für Sie und uns. WatchGuard legt den Fokus zu 100 Prozent auf den Channel, und das schon seit über 20 Jahren. Unsere gesamte Organisation ist auf Ihren Erfolg ausgerichtet, einschließlich wie wir Produkte entwerfen und entwickeln, Services bündeln und verkaufen sowie Ihr Unternehmen unterstützen. Wir spielen in der Channel-Entwicklung ganz vorne mit.

Maximale Rentabilität

Bei WatchGuardONE geht es vor allen Dingen um Ihre Profitabilität. Sie profitieren von Frontend-Rabatten, Backend-Boni, Deal Registration, Kooperationszuschüssen, Werbekostenzuschüssen, SPIFF-Programmen und mehr. Sie werden kaum ein attraktiveres Programm finden.

Je mehr Sie lernen, desto mehr können Sie verdienen

WatchGuardONE schätzt Ihren Aufwand als Sicherheitspartner wert. Anders als die üblichen umsatzbasierten Programme im IT-Vertrieb ist unser Technologiepartnerprogramm darauf ausgerichtet, Ihr Engagement für WatchGuard und die von uns gemeinsam angebotenen

Lösungen zu belohnen. Durch unsere einzigartigen WatchGuardONE-Spezialisierungen können Sie umso mehr Rabatte erhalten, je mehr Zeit und Aufwand Sie in WatchGuardONE investieren.

Unterstützung unterschiedlicher Geschäftsmodelle

Unabhängig von Unternehmensgröße und Markteinführungsstrategie weiß WatchGuard Ihr Unternehmen bei einer Partnerschaft zu schätzen. Unsere Channel Community umfasst einige der vielseitigsten IT-Lösungsanbieter, einschließlich Vertriebspartnern, VARs, Beratern, Systemintegratoren, MSPs, MSSPs und der vielen verschiedenen hybriden Modelle dazwischen. Außerdem bieten wir produktspezifische Spezialisierungen in den Bereichen Network Security, Secure Wi-Fi, Multifaktor-Authentifizierung und Endpoint-Sicherheit. So können Sie eine personalisierte Partnerschaft aufbauen, die auf die Produkte und Dienste ausgerichtet ist, auf denen Ihr geschäftlicher Fokus liegt. Für eine umfassende Einführung der Cybersicherheits-Plattform von WatchGuard erhalten Sie mehr Anerkennung und Anreize.

Ein zuverlässiger Partner

Als WatchGuardONE Partner wird Ihnen ein festes Account-Management-Team zugewiesen, das Sie bei der Suche nach neuen Geschäftsmöglichkeiten und beim Aufbau Ihres Unternehmens unterstützt. Sie können flexible Preisoptionen nutzen, erhalten eine Reihe von Tools und Ressourcen für das Channel Enablement, haben vorrangigen Zugang zu unserem preisgekrönten technischen Support-Team und vieles mehr!



Das WatchGuard-Portfolio



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.



Sicheres WLAN

Die sicheren WLAN-Lösungen von WatchGuard sind eine richtungsweisende Neuerung für den Markt von heute: Sie schaffen eine sichere, geschützte WLAN-Umgebung, eliminieren den Verwaltungsaufwand und ermöglichen beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.



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.



Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein cloudnatives, 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.

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 asiatisch-pazifischen Raum.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333

INTERNATIONALER VERTRIEB: +1 206 613 0895

WEB www.watchguard.de