
Intelligente Sicherheit
leicht gemacht.
WatchGuard®

Seit über 25 Jahren

Wegbereiter in puncto Cybersicherheit

1996 gegründet

Firmensitz: Seattle, Washington

7 Einsatzzentralen und Direktvertretungen in **21** Ländern

Über 1.200 Mitarbeiter

Über 250K+ Kunden

Über 100+ Distributoren

Über 16.000 aktive Vertriebspartner

2018 – Einführung von DNSWatch

2019 – Einführung von WatchGuard Cloud für MSPs

'18 '19 '20

2018 – Einführung des AuthPoint MFA

2019 – Erweiterung der DNS-Filter auf Clients außerhalb des Netzwerks mit DNSWatchGO

2020 – Erweiterte Endpunktsicherheit hinzugefügt

WatchGuard ist seit über 25 Jahren Wegbereiter bei der Entwicklung innovativer Cybersicherheitstechnologie und stellt sie in einer benutzer- und verwaltungsfreundlichen Lösung bereit. Durch branchenführende Netzwerksicherheit, sicheres WLAN sowie Produkte und Dienstleistungen im Bereich der Network Intelligence ermöglicht WatchGuard über 80.000 Kunden weltweit den Schutz ihrer wichtigsten Ressourcen – in einer Welt, in der die Zahl neuer Bedrohungen in der Cybersicherheitslandschaft tagtäglich wächst.

Intelligente Sicherheit leicht gemacht.

WISSENSWERTES ZUM THEMA CYBERSICHERHEIT

Cybersicherheit ist ein komplexes Thema, und die Technologien, die zum Schutz vor Cyberkriminellen genutzt werden, werden immer ausgereifter. Es geht darum, all diese Technologien zu bündeln und sie kleinen und mittelständischen Unternehmen, die keine eigenen Sicherheitsteams beschäftigen, in einem anwenderfreundlichen Paket an die Hand zu geben. Es geht außerdem 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.

EINFACHHEIT

Kauf, Konfiguration, Bereitstellung und zentrale Verwaltung – ganz problemlos

INNOVATION

Schneller Zugriff auf neue und verbesserte Sicherheitsdienste

LEISTUNG

Höchste UTM-Leistung in jeder Preislage

VISUALISIERUNG

Konvertierung unzähliger Daten in verwertbare Informationen über einfache Berichterstellung und Korrelation von Bedrohungen

SUPPORT

Branchenführender Pre- und Post-Sales-Support für maximale Kunden- und Partnerzufriedenheit

Das heutige Wirtschaftsumfeld ist auf das Internet angewiesen, das IT-Umgebungen und Standorte aller Art umspannt. Dabei bringt jede ihre eigenen Anforderungen an Cybersicherheit mit. Ob Sie physische oder virtuelle Infrastrukturen, Netzwerke, Endpunkte oder WLAN-Umgebungen an einem oder mehreren Standorten schützen müssen: WatchGuard erlaubt Ihnen ein wirksames, unternehmensweites Sicherheitsmanagement.

Sicherheit auf Enterprise-Niveau für Unternehmen von heute

Ein mehrschichtiger Sicherheitsansatz

Schieben Sie unbefugtem Datenzugriff, der Ausbeutung anfälliger Systeme, ausgereifter Malware und dem Ausschleusen persönlicher Daten einen Riegel vor. WatchGuard sprengt die Fesseln der Cyber Kill Chain® in jeder Bedrohungsphase – durch einen mehrschichtigen Sicherheitsansatz, intelligente Abwehr, die Erkennung von und Reaktion auf Bedrohungen, die gezielte Angriffe im Keim ersticken.

RECHERCHE
Der Angreifer sammelt Informationen über das Opfer

ÜBERMITTLUNG
Der Angreifer übermittelt die Angriffsnutzlast über den Netzwerkperimeter

KOMPROMITTIERUNG/EXPLOIT
Im Rahmen der Recherche identifizierte Schwachstellen werden zu Angriffszwecken ausgenutzt

INFIZIERUNG/INSTALLATION
Die Nutzlast wird im System installiert, wo sie sich einnistet

STEUERZUGRIFF
Die Nutzlast wartet auf Anweisungen des Angreifers

LATERALE BEWEGUNG
Der Angreifer arbeitet sich innerhalb des Netzwerkperimeters an das Endziel heran

ANGRIFFSZIEL ERREICHT/EXFILTRATION
Das Angriffsziel wurde erreicht

Best-in-Class Sicherheitsdienste

WatchGuard bietet das umfassendste Portfolio von Netzwerksicherheitsdiensten auf dem Markt an: von traditionellem IPS über GAV, Application Control, Spam-Abwehr und Web-Filtern bis hin zu weiterführenden Diensten, die vor ausgereifter Malware, Ransomware und dem Verlust sensibler Daten schützen. Abgerundet wird das Angebot von WatchGuard durch ein Komplettpaket mit Diensten für die Netzwerkvisualisierung und -verwaltung.

Grundlegende Sicherheitsdienste

Intrusion Prevention Service (IPS)
Dieser Dienst überwacht mithilfe laufend aktualisierter Signaturen den Datenverkehr in allen gängigen Protokollen und bietet Echtzeit-Schutz vor Netzwerkbedrohungen.

Reputation Enabled Defense (RED)
Ein cloudbasierter Reputations-Suchdienst, der Benutzer vor bösartigen Websites und Botnets schützt und dabei den Overhead bei der Webverarbeitung erheblich verbessert.

Application Control
Mit diesem Feature können Sie den Zugriff auf Anwendungen in Abhängigkeit von Abteilung, Position im Unternehmen und Tageszeit gewähren, verweigern oder einschränken. Anschließend verfolgen Sie in Echtzeit, was von wem aufgerufen wurde.

spamBlocker
Spam wird in Echtzeit erkannt, bevor er massenhaft um sich greifen kann. Dabei ist spamBlocker ultraschnell – und äußerst effektiv: Tagtäglich werden bis zu vier Milliarden Nachrichten überprüft.

WebBlocker – URL Filterung
Blockiert bösartige Websites automatisch; durch Einsatz granularer Content-Filter-Tools können unangemessene Inhalte blockiert und die Produktivität gesteigert werden.

Network Discovery
Ein abonnementbasierter Dienst, der eine visuelle Topologie sämtlicher Knoten in Ihrem Netzwerk generiert. So können Sie umgehend riskante Bereiche erkennen.

Gateway Antivirus (GAV)
Laufend aktualisierte Signaturen identifizieren und blockieren bekannte Spyware, Viren, Trojaner und mehr – einschließlich neuer Varianten bekannter Viren.

Erweiterte Sicherheitsdienste

APT Blocker – erweiterter Schutz vor Schadsoftware
Durch Einsatz einer prämierten Sandbox der nächsten Generation werden selbst raffinierteste Attacken erkannt und gestoppt, einschließlich Ransomware und Zero-Day-Angriffen.

Threat Detection and Response
Setzen Sie Sicherheitsereignisse im Netzwerk und am Endpunkt in Bedrohungsanalysen in Beziehung. Dadurch können potenzielle Angriffe noch früher erkannt, priorisiert und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung.

IntelligentAV™
IntelligentAV ist eine signaturlose Anti-Malware-Lösung, die künstliche Intelligenz zur automatischen Erkennung von Schadsoftware einsetzt. Durch Nutzung umfassender statistischer Analysen kann aktuelle und Zero-Day-Schadsoftware in Sekundenschnelle klassifiziert werden.

DNSWatch™
Verringert Infektionen durch Schadsoftware, indem bösartige DNS-Anforderungen blockiert und Benutzer zu Informationen umgeleitet werden, die ihnen Best Practices in puncto Sicherheit vermitteln und betonen, wie wichtig deren Einhaltung ist.

EINE BENUTZERFREUNDLICHE, KOSTENEFFEKTIVE LÖSUNG

Alle Sicherheitsdienste von WatchGuard werden als integrierte Lösung über eine benutzerfreundliche und kosteneffektive Firebox®-Appliance bereitgestellt, die als physische und virtuelle Instanz erhältlich ist. Mit WatchGuard müssen Sie sich nie zwischen Sicherheit und Leistung entscheiden. Jede Firebox-Appliance enthält ein komplettes Portfolio von Sicherheitsdiensten und eine Reihe von Management- und Visualisierungswerkzeugen, mit der Sie der schnell wachsenden Bedrohungslage immer einen Schritt voraus bleiben. Sobald neue Technologien verfügbar sind, können Sie Ihre Software problemlos aktualisieren, um die neuesten Angebote zu integrieren.

REIBUNGSLOSE ANSCHAFFUNG

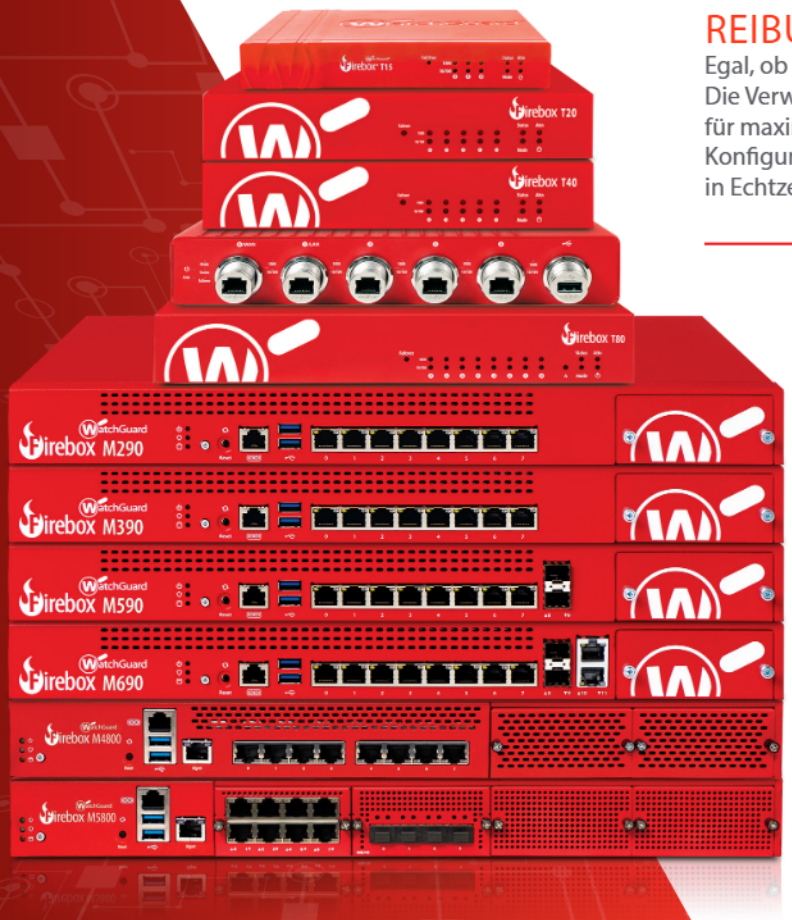
Eine Plattform, ein Paket, umfassende Sicherheit. Unsere Sicherheitsplattform verbindet intelligente, branchenführende Korrelation mit einer umfassenden Auswahl leistungsstarker Dienste für höchste Sicherheit im Netzwerk und am Endpunkt.

REIBUNGSLOSE BEREITSTELLUNG

Mit unserem cloudbasierten Bereitstellungs- und Konfigurationswerkzeug lassen sich mehrere Firebox®-Appliances an dezentralen Standorten jederzeit fernkonfigurieren und mit minimaler Unterstützung vor Ort einrichten.

REIBUNGSLOSE VERWALTUNG

Egal, ob eine oder Hunderte Firebox-Appliances:
Die Verwaltung erfolgt über eine benutzerfreundliche Konsole – für maximale Effizienz und eine schlanke Netzwerkadministration. Konfigurationsänderungen können planmäßig oder in Echtzeit erfolgen.



Eine Plattform, umfassende Sicherheit

Abgestimmt auf Ihren Bedarf

Nur die Funktionen, die Sie tatsächlich benötigen

Unsere Sicherheitsservicepakete ermöglichen Ihnen die schnelle und einfache Auswahl der richtigen Funktionen für Ihre Geschäftsbedürfnisse von heute – und morgen.

SUPPORT

Neben statusbehafteten Firewalls umfasst die Support-Lizenz vollständige VPN-Funktionalität und ein integriertes SD-WAN.

BASIC SECURITY

Die Basic Security Suite umfasst alle traditionellen Netzwerk-Sicherheitsservices, die für ein UTM-Gerät üblich sind: IPS, Antivirus, URL-Filterung, Application Control, Spam-Schutz und Reputations-Suche. Sie enthält darüber hinaus auch zentralisierte Management- und Netzwerkvisualisierungsfunktionen sowie unseren Support, der standardmäßig rund um die Uhr verfügbar ist.

TOTAL SECURITY

Die Total Security Suite verfügt neben sämtlichen Services der Basic Security Suite über KI-Malware-Schutz, erweiterte Netzwerkvisualisierungsfunktionen, Endpunktschutz, Cloud-Sandboxing, DNS-Filter sowie Mechanismen zur Abwehr von Bedrohungen direkt aus WatchGuard Cloud, unserer Netzwerkvisualisierungsplattform.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service)IPS)		✓	✓
Anwendungskontrolle		✓	✓
WebBlocker (URL-/Inhaltsfilterung)		✓	✓
spamBlocker (Anti-Spam)		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
ThreatSync			✓
DNSWatch			✓
IntelligentAV*			✓
WatchGuard Cloud Visibility Datenaufbewahrung		1 Tag	30 Tage
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

*Total Security Suite erforderlich für Firebox V und Firebox Cloud.

Fundierte Entscheidungen durch Erkennung bekannter Muster

UMGEHEND VERWERTBARE SICHERHEITSINFORMATIONEN AUS EINER FLUT VON PROTOKOLLDATEN

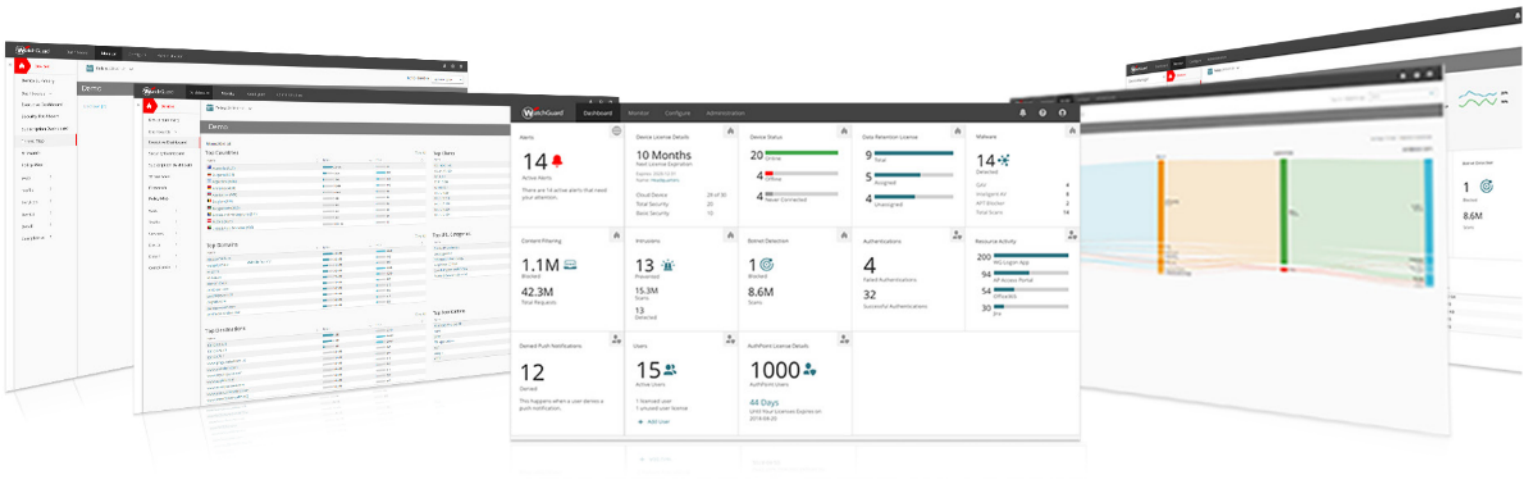
Wenn Sie nicht sehen können, was in jedem Winkel Ihrer IT-Infrastruktur vor sich geht, dürfen Sie das nicht auf die leichte Schulter nehmen. Diese toten Winkel stellen ein massives Sicherheitsrisiko dar. WatchGuard ermöglicht Ihnen eine umfassende Visualisierung Ihres gesamten Netzwerks. Dies erreichen 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 Richtliniennutzung, Compliance, Netzwerk- und Datenverkehr, Sicherheitsdienste, Dialog-, Benutzeranalysen und Gerätestatistiken informieren. Berichte sind jederzeit abrufbar und können im Rahmen vorbeugender und korrektiver Maßnahmen automatisch zugestellt werden.



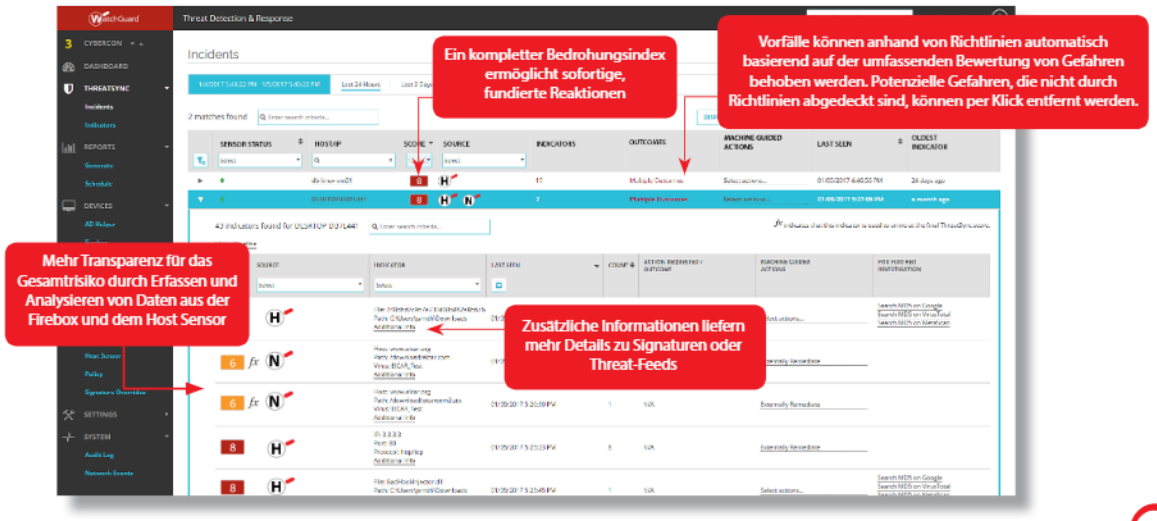
WatchGuard Cloud Visibility

SO FÜGT SICH ALLES ZUSAMMEN

Ganz egal, welche Sicherheitslösungen Sie einsetzen: Wenn Sie keinen Kontext für Ihre Daten schaffen, kann Ihr Unternehmen weiterhin in Gefahr sein. Korrelation fügt die einzelnen Informationen aller Sicherheitsdienste zusammen, damit diese einen gemeinsamen Sinn ergeben. Durch die umfassende Betrachtung von Endpunkt und Netzwerk lässt sich besser einschätzen, welche Bedrohungen am gefährlichsten sind.

ThreatSync ist die cloudbasierte Engine von WatchGuard zur Korrelation und Bewertung von Bedrohungen. Mit ihrer Hilfe profitieren Unternehmen von einem erhöhten Sicherheitsbewusstsein sowie maximaler Reaktionsfähigkeit gegenüber Gefahren innerhalb des gesamten Netzwerks – bis zum Endpunkt. ThreatSync erfasst Ereignisdaten der Sicherheitsdienste von WatchGuard innerhalb des Netzwerks. Es setzt die Daten zu von WatchGuard Host-Sensoren erkannten Bedrohungsaktivitäten und intelligenter Gefahrenerkennung auf Enterprise-Niveau in Beziehung. ThreatSync informiert Sie anhand einer umfassenden Bedrohungsanalyse über Einstufung und Schweregrad von Bedrohungen.

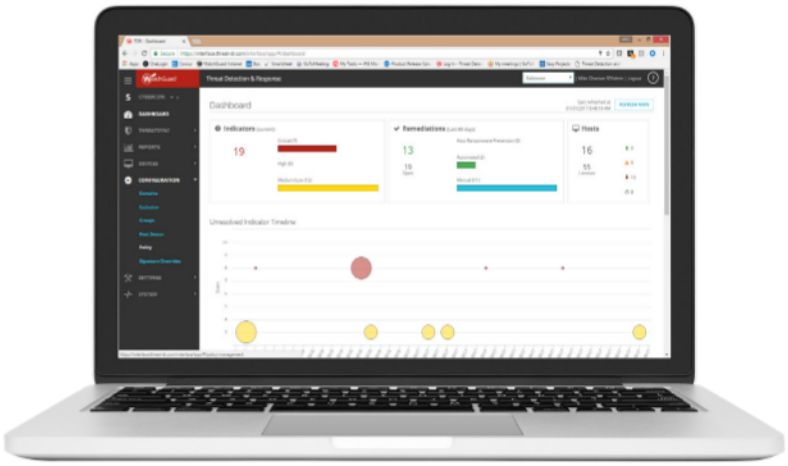
Diese proprietäre Technologie verbessert nicht nur die Visualisierung von Bedrohungen am Endpunkt und im Netzwerk und sorgt auf diese Weise für eine schnellere Gefahrenerkennung – sie ermöglicht außerdem eine zeitnahe und effektive Reaktion. Sie beschleunigt die Gefahrenabwehr, bietet eine messbare Rentabilität und senkt den für den Schutz Ihres Unternehmens benötigten Zeit- und Ressourcenaufwand.



WatchGuard Threat Detection and Response

Zögern Sie nicht und automatisieren Sie

Automatisierung steht im Mittelpunkt der einheitlichen Sicherheitsplattform von WatchGuard. 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. 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 dauerhaften, 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.



Stufe 1: Management und Visualisierung	Signatur- und Softwareupdates	Sofort nutzbare Berichte und Dashboards		Sichere Firewall-Standardeinstellungen
Stufe 2: Betrieb	Cloud-Bereitstellung	Lizenzmanagement	Verarbeitung von Rechnungen und Support-Tickets	Integration von APIs und Webdiensten
Stufe 3: Reaktionsschnelle Sicherheit	Verhaltensbasierte und statistische Modellierung	Abhilfe	Korrelation von Bedrohungen	Isolierung von Endpunkten
Stufe 4: Prädiktive Sicherheit	KI-gestützte Prävention, Erkennung, Sichtung und Abhilfe			

Der WatchGuard Automation Core bietet:

WIRKSAMKEIT DER SICHERHEITSMASSNAHMEN

- Im Jahr 2019 hat eine Firebox im Durchschnitt über 2.100 Malware-Varianten blockiert. Rund 40 % davon wurden als Zero-Day-Malware eingestuft, d. h. sie blieben bei Anwendung der signaturbasierten Methode komplett unerkannt.[1] Zudem hat jedes Gerät durchschnittlich 240 weitere Netzwerkangriffe abgewehrt.
- Bei den Tests von NSS Labs erwies sich WatchGuard als eine von nur zwei Firewall-Plattformen, denen KEIN Ausweichmanöver entgangen war. WatchGuard hat in drei aufeinanderfolgenden Jahren die Bewertung „Recommended" (Empfohlen) erhalten.

ERWEITERBARKEIT

- Schützen Sie Ihre Anwender innerhalb und außerhalb des Netzwerks vor Phishing 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 anmelden oder vom Netzwerk abmelden.

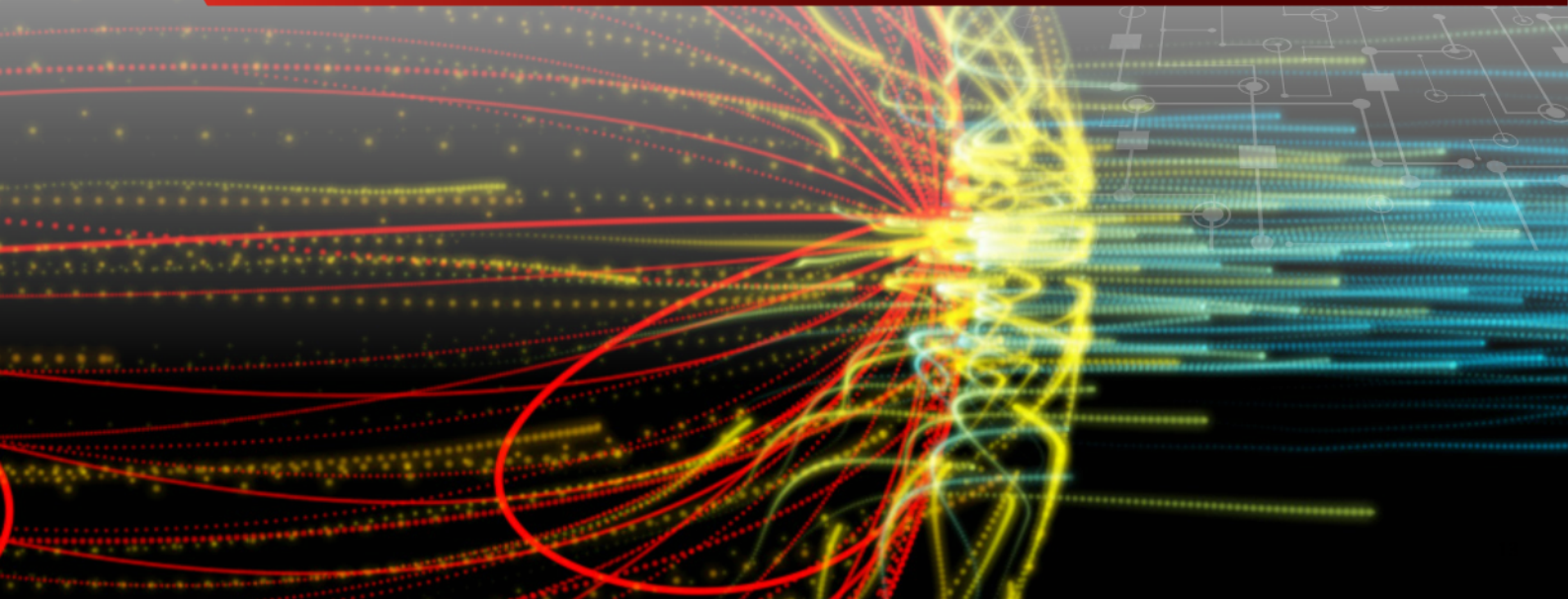
STÄRKERE AUSLASTUNG DES IT-PERSONALS

- Bei über 12.000 Bereitstellungen wurde unser Cloud-Dienst RapidDeploy in Anspruch genommen. Dabei wurde nur ein Hundertstel der Zeit und Kosten aufgewendet, die bei einer standardmäßigen Geräteeinrichtung und -konfiguration anfallen.
- Die leistungsstarken Transparenztools von WatchGuard warten mit über 100 vorgefertigten Dashboards und Berichten auf. Damit sparen Sie mehrere Hundert Stunden im Vergleich zum Durchsuchen von Protokollen nach zeitkritischen Nutzungs- und Anomaliedaten.
- Zeit und Geld sparen
- Mittels KI weist die Firebox-Plattform auf Bedrohungen hin, bis zu 33 Monate bevor sie in den freien Umlauf gelangen.[2]
- Sollten Angriffe bis zum Netzwerk vordringen, ermöglicht wir die Früherkennung verdächtiger Verhaltensweisen. Wo Bedrohungen vorher monatelang im Netzwerk existierten, werden sie jetzt innerhalb von wenigen Minuten automatisch eingedämmt und beseitigt.

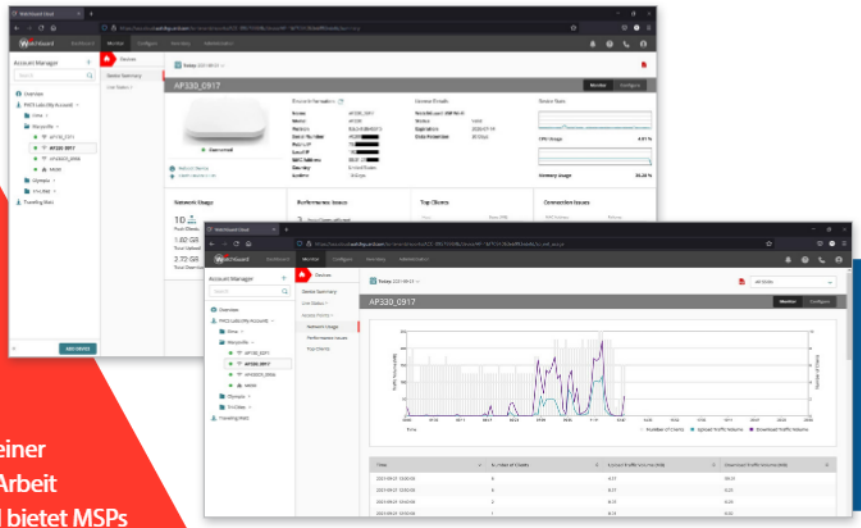
Aber das ist noch nicht alles! Wir wissen, dass Sie eine hoch automatisierte Sicherheitserfahrung erwarten, die Sicherheitsexpertise, aktuelle Überwachung und Sicherheitsoptimierungen beinhaltet. Halten Sie nach weiteren Automation Core-Verbesserungen Ausschau, die das Markenzeichen zukünftiger Produktinnovationen von WatchGuard sind.

1 https://www.watchguard.com/wgrd-resource-center/security-report-q2-2019
2 https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SELabsPredictiveMalwareResponseTestMarch2018Report.pdf

WatchGuard Automation Core



Vereinfachtes WLAN in WatchGuard Cloud



Der Bedarf an drahtloser Kommunikation hat sich zu einer Notwendigkeit entwickelt, um Konnektivität in der Arbeit und Freizeit zu sichern. Wi-Fi in WatchGuard Cloud bietet MSPs eine vereinfachte Möglichkeit, mehrere Sicherheitsdienste über verschiedene verteilte Arbeitsgruppen hinweg zentral zu verwalten, was der Mission von WatchGuard entspricht, eine einheitliche Security-Plattform aufzubauen.

ZERO-TOUCH-BEREITSTELLUNG

Wi-Fi 6-Access Points erleichtern die Einarbeitung von Mitarbeitern durch einfach einzurichtende Geräte, die nicht von den IT-Teams des Unternehmens persönlich installiert werden müssen.

REPORTING UND VISUALISIERUNG

MSPs verfügen nun über transparenten Einblick in wichtige Informationen wie Signalstärken-Reichweite, Bandbreitenverbrauch des WLAN-Clients, Nutzung von Access Points und Client Distribution, um den durchgängigen, vollständigen Überblick über Gerätezustand und -system zu gewährleisten.

MULTI-TIER- UND MULTI-TENANT-FUNKTIONEN

Mit Wi-Fi in WatchGuard Cloud lassen sich WLAN-Verbindungen und -Leistung für die einzelnen Nutzer unkompliziert auf nur einer Plattform bereitstellen, konfigurieren und dokumentieren, um die komplexe Verwaltung mehrerer Dienste zu vereinfachen.

SICHERE WLAN-FUNKTIONEN

Unsere Wi-Fi 6-Access Points bieten Wi-Fi 6-Technologie und WPA3-Verschlüsselung in nur einem Wireless Access Point. Mit dem Wechsel von WLAN-Bestandsnetzwerken zu Firmen- und persönlichen Netzwerken, die anders als frühere WLAN-Versionen intelligent einen umfassenden Bereich abdecken, können IT-Teams und MSPs Endanwender zuverlässig vernetzen.

SICHERHEIT AUF ENTERPRISE-NIVEAU

WatchGuard bietet Schutz vor WLAN-Cyberbedrohungen, indem es verdächtige Schadsoftware blockiert, Eindringversuche unterbindet und schädliche Inhalte filtert und so die Angriffsfläche minimiert.

VEREINFACHTE VERWALTUNG MIT EINER EINHEITLICHEN SECURITY-PLATTFORM

Wi-Fi in WatchGuard Cloud ermöglicht es IT-Managern und MSPs in Unternehmen, die Leistung des Ökosystems von Geräten, die mit dem Unternehmensnetzwerk verbunden sind, in Echtzeit über ein einziges Portal zu diagnostizieren, zu überwachen und Berichte zu erstellen, um eine einheitliche Sicht zu gewährleisten. Die Lösung wurde nativ für das WatchGuard-Security-Produktportfolio konzipiert, um die Verwaltung für WatchGuard-Bestandskunden zu optimierenund den IT-Aufwand zu verringern.

Die Wi-Fi 6-APs bieten hohe Geschwindigkeiten und umfassende Sicherheit. Wi-Fi 6 und WPA3 sind für ein modernes Netzwerk unerlässlich und WatchGuard hat ein außergewöhnliches WLAN-Erlebnis geschaffen.

~ Luis Gimenez, Director of Technology bei SPW

Multifaktor-Authentifizierung mit AuthPoint

Die Verwendung gestohlener Anmeldedaten, um unerlaubt auf Netzwerkressourcen zuzugreifen, ist die beliebteste Taktik von Hackern.*

**Verizon Data Breach Investigations Report 2018*

AuthPoint hält das Versprechen der MFA. Die App reduziert das Geschäftsrisiko von schwachen Passwörtern, ohne die Benutzerfreundlichkeit für Mitarbeiter und IT-Personal zu beeinträchtigen. Alles in einem Cloud-Dienst – ohne Hardware-Installation und Verwaltung von Software…MFA wird heutzutage als unerlässlich betrachtet und ist bei WatchGuard problemlos verfügbar.
~ Tom Ruffolo, CEO, eSecurity Solutions

KOMPLETT CLOUDVERWALTET

AuthPoint wird auf der WatchGuard Cloud-Plattform ausgeführt und ist überall verfügbar. Sie müssen keine Software installieren, Upgrades planen oder Patches verwalten. Die Plattform stellt eine Ansicht eines einzelnen globalen Accounts oder vieler unabhängiger Accounts einfach bereit, sodass dezentrale Unternehmen und Managed Service Provider nur die Daten anzeigen können, die für die Rolle einer Person relevant sind.

EFFIZIENTER MFA-SCHUTZ ÜBER DNA DES MOBILGERÄTS

AuthPoint bietet ein sicheres MFA-Produkt mit 3 Möglichkeiten der Authentifizierung. Ferner gleicht unsere Mobilgeräte-DNA das autorisierte Smartphone des Benutzers ab, wenn Zugriff auf Systeme und Anwendungen gewährt wird. Jeder Angreifer, der versucht, sich mit geklonten Authentifizierungsmeldungen Zugriff zu verschaffen, wird blockiert, wenn die Meldungen nicht vom Smartphone des legitimen Benutzers stammen.

BENUTZERFREUNDLICHE MOBILE AUTHPOINT-APP

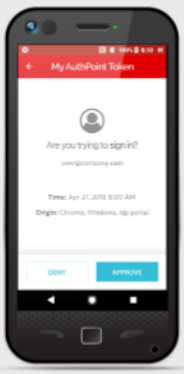
Benutzer können sich direkt über ihr Smartphone authentifizieren. Sie benötigen keine Key Fobs oder USB-Sticks, sondern können stattdessen die mobile AuthPoint-App in Sekundenschnelle installieren und aktivieren. Die App ermöglicht eine schnelle Push-basierte Authentifizierung sowie Offline-Authentifizierung mit QR-Codes über die Smartphone-Kamera.

UMFASSENDE ABDECKUNG MIT WEB-SSO

Unser Ökosystem umfasst Dutzende von Drittanbieterintegrationen. Unternehmen können Benutzer also auffordern, sich zu authentifizieren, bevor sie auf sensible Cloud-Anwendungen, VPNs, Web Services und Netzwerke zugreifen. AuthPoint unterstützt zudem den SAML-Standard, der es Benutzern ermöglicht, mit einer einzigen Anmeldung auf eine breite Palette von Anwendungen und Diensten zuzugreifen. Die sichere Anmeldefunktion ermöglicht Online- und Offline-Authentifizierung bei Windows- oder Mac-Rechnern unter Verwendung der AuthPoint-App.

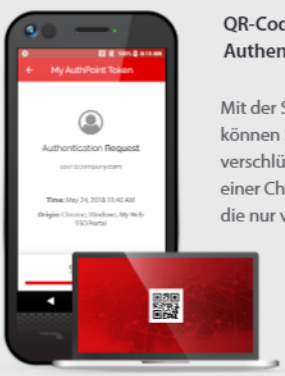
Google Dropbox GoToMeeting Microsoft Office 365 OPENVPN Firebox

DREI MÖGLICHKEITEN ZUR AUTHENTIFIZIERUNG



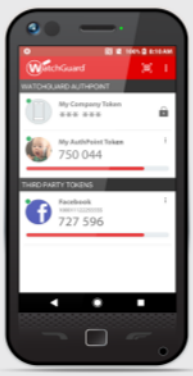
Push-basierte Authentifizierung

Sichere Authentifizierung mit One-Touch-Genehmigung. Sie sehen, wer sich authentifizieren möchte (inkl. seines Standorts), und Sie können nicht autorisierten Zugriff auf Ihre Ressourcen blockieren.



QR-Code-basierte Authentifizierung

Mit der Smartphone-Kamera können Sie einen eindeutigen, verschlüsselten QR-Code mit einer Challenge einlesen, die nur von der App gelesen werden kann. Die passende Antwort für den Abschluss der Authentifizierung ist bereits enthalten.



Zeitbasiertes Einmalpasswort (One-Time Password, OTP)

Ein dynamisches, zeitbasiertes Einmalpasswort wird abgerufen und – wie angezeigt – bei der Anmeldung eingegeben.

WatchGuard Endpoint-Sicherheitmit

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-Sicherheit 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-Sicherheit. 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 Ermittlungen gestützt und führen Bedrohungssuchen und eine 100-prozentige Klassifizierung von Anwendungen durch. Dadurch wird die Legitimität und Sicherheit aller ausgeführten Anwendungen zertifiziert, eine entscheidende Anforderung für jedes Unternehmen, das ein Zero-Trust-Sicherheitsmodell implementiert.

GUT ODER SCHÄDLICH? ZU 100 PROZENT VERLÄSSLICHE ANTWORTEN

Die meisten Sicherheitsprodukte für Endpoints 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 (Endpoint Protection, Detection and Response) hingegen bieten einen Zero Trust Application Service, der ausführbare Dateien zu 100 % klassifiziert. Dazu werden alle verdächtigen und unbekannten Prozesse und Anwendungen mithilfe spezieller KI-Algorithmen in unserer Cloudplattform analysiert und bei Bedarf sogar von unseren Labortechnikern verifiziert. 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.

ERWEITERUNG DER SICHERHEIT, DER TRANSPARENZ UND DER EINSATZFÄHIGKEITEN

Zu den optionalen Modulen gehört das Patch Management, mit dem Updates und Patches für Betriebssysteme, Drittanbieteranwendungen und nicht mehr unterstützte Softwareprogramme (EOL-Software) zentral verwaltet werden, die Full Encryption, mit der Daten der Endpoints verschlüsselt und entschlüsselt werden, unser Advanced Reporting Tool, um Sicherheitsinformationen zusammenzustellen und Angriffe und ungewöhnliches Verhalten zu identifizieren, und Data Control, um unstrukturierte personenbezogene Daten, die auf Endpoints gespeichert sind, zu entdecken, zu klassifizieren, zu prüfen

Erweiterte Endpoint Security

und zu überwachen. SIEM Feeder überwacht alle Prozesse, die auf Ihren Geräten ausgeführt werden, und stellt eine neue Quelle für wichtige Informationen dar. Systems Management, unser RMM-Tool, verwaltet, überwacht und wartet Ihre gesamte IT-Infrastruktur.

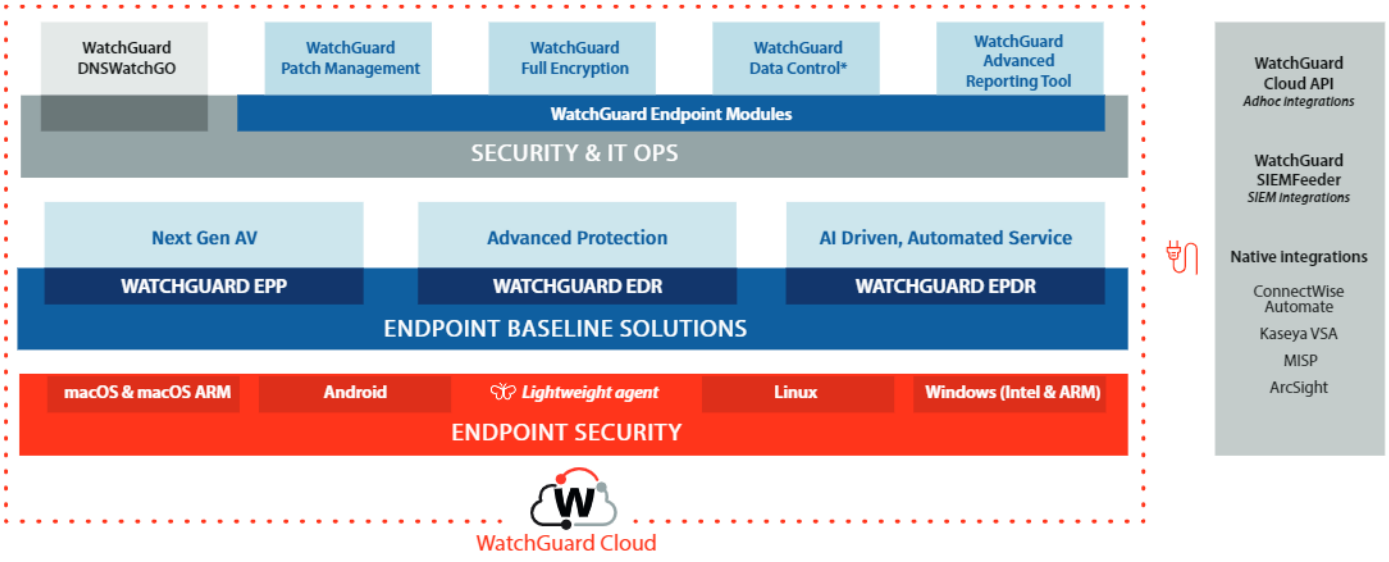
LAUERNDE BEDROHUNGEN OHNE ZUSÄTZLICHES PERSONAL FINDEN

Die Bedrohungssuche erfordert in der Regel hoch qualifizierte Ressourcen und nimmt viele Stunden in Anspruch, bevor die Gefahren aufgespürt und Erkenntnisse gewonnen werden, die dabei helfen, die Bedrohungen zu beseitigen. 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 CLOUDBASIERTEM MANAGEMENT

Unternehmen mit wenigen IT-Mitarbeitern und geringem Sicherheits-Know-how profitieren von WatchGuard Cloud. Diese cloudbasierte 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

EIN KOMPLETTPAKET MIT FLEXIBLEN OPTIONEN FÜR JEDEN BEDARF



Das sagen unsere Kunden

> Wir haben uns für WatchGuard entschieden, weil es das einzige Produkt auf dem Markt war, das alle Funktionen bot, die wir an sämtlichen Standorten benötigten, ohne unser Budget zu sprengen.
>
> ~ Neil MacGregor, IT-Leiter, Warren Evans

Fallstudien

„Durch den Einsatz des WatchGuard Reputation-Authority-Filters, der Application Control und des WebBlockers profitieren wir von einer verbesserten Internetsicherheit und schützen unsere Anwender vor der wachsenden Zahl potenzieller, eingehender Bedrohungen. Auch der Mobilitätssupport für Laptops und Smartphones ist umfassender, das wird zunehmend wichtiger …. Ich nutze WatchGuard seit vielen Jahren und sehe keinen Grund, das zu ändern. Warum sollen wir auf eine andere Appliance umsteigen, wenn die, die wir haben, sämtliche Anforderungen erfüllt und noch mehr kann."

~ Gary Lovelock, IT-Manager, Marshall Amplification

„Unsere Marke ist der Schlüssel zum Erfolg unseres Unternehmens, die Wahrung unseres Renommees ist für uns daher von entscheidender Bedeutung. Die Netzwerksicherheit und der Schutz unserer digitalen Ressourcen und Datenbanken hat absolute Priorität….WatchGuard hat unsere Erwartungen eindeutig übertroffen. Sie haben nicht nur erstklassige Firewalls zu bieten, neue Firmware-Releases enthalten fortwährend Verbesserungen. Sie bieten reichhaltige Funktionen und Wertschöpfungskomponenten – etwa den System Manager und Dimension – ich kenne keine anderen Anbieter, die diese mit ihren Produkten bündeln. WatchGuard kann ich eindeutig weiterempfehlen."

~ Richard Isted, IT-Manager, The Ritz London

„Da sowohl unsere finanziellen als auch personellen Möglichkeiten begrenzt waren, hatten wir nicht viel Spielraum und mussten umso effizienter agieren. Mit WatchGuard hat sich das grundlegend verändert…. Wir sind mit den Produkten zufrieden, vom Support begeistert und es gab in puncto Sicherheit niemals irgendein Problem, das wir mit WatchGuard nicht lösen konnten."

– Hunter Hughes, IT-Leiter, Museum of Flight

PRODUKTINTEGRATIONEN FÜR INTELLIGENTERE SICHERHEIT

WatchGuard ONE TECHNOLOGY PARTNER

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. WatchGuard deckt alles ab – von Authentifizierungsprodukten, über Servicemanagement-Plattformen, Visualisierungslösungen bis hin zu Cloud-Diensten. Und wir gehen immer neue Geschäftspartnerschaften ein, um die gefragtesten und innovativsten Integrationen anbieten zu können. Jede Integration wird verifiziert und in einem Integrationsleitfaden dokumentiert, der Schritt für Schritt durch die Konfiguration führt.

EIN VERTRIEBSPARTNER FÜR INDIVIDUELLE ANFORDERUNGEN

WatchGuard ONE CHANNEL PARTNER

WatchGuard unterhält die engagierteste und fachkundigste Vertriebspartnergemeinschaft der Branche. Seit über 20 Jahren schaffen wir eine erstklassige Channel-Grundlage, um Kunden mit den richtigen Geschäftspartnern zusammenzubringen und ihren Erfolg von Anfang an zu sichern. Ob Sie nach einem allgemeinen Vertriebspartner suchen oder ergänzend zum Kauf von Produkten ein durchgängiges Servicemanagement benötigen: Wir helfen Ihnen bei der Auswahl des perfekten Partners. All unsere Vertriebspartner werden im Rahmen unseres WatchGuardONE-Programms geschult und zertifiziert und stehen Ihnen gerne als Sicherheitsexperten zur Seite.

Ein zweckbestimmter Channel zertifizierter Partner

SCHÜTZEN SIE IHR UNTERNEHMEN • SCHÜTZEN SIE IHRE RESSOURCEN • SCHÜTZEN SIE IHRE MITARBEITER

Cybersicherheit ist heute relevanter denn je. Die Anzahl der weltweiten Cyberangriffe hat einen Höchststand erreicht – und es gibt keine Anzeichen für einen Rückgang. Kleine und mittelständische Unternehmen fallen diesen Angriffen, die schwerwiegende Auswirkung auf betriebliche Vorgänge und auf die Geschäftskontinuität haben, weiterhin zum Opfer. WatchGuard bietet Ihnen den erforderlichen mehrschichtigen Schutz vor der raffiniertesten Malware und macht Ihnen die Verwaltung leicht. Sie sind den gleichen Bedrohungen ausgesetzt wie Großunternehmen, sollten Sie dann nicht auch vom gleichen Sicherheitsniveau profitieren?

Globale Hauptgeschäftsstelle USA
Tel: +1.206.613.6600
E-Mail: sales@watchguard.com

Hauptgeschäftsstelle Central Europe
Tel: +49 (700) 9222 9333
E-Mail: germanysales@watchguard.com

Hauptgeschäftsstelle APAC-Ozeanien Singapur
Tel: +65.3163.3992
E-Mail: inquiry.sea@watchguard.com