


Einsatz von Zero-Trust-Netzwerken im Zeitalter von COVID-19

WatchGuard®

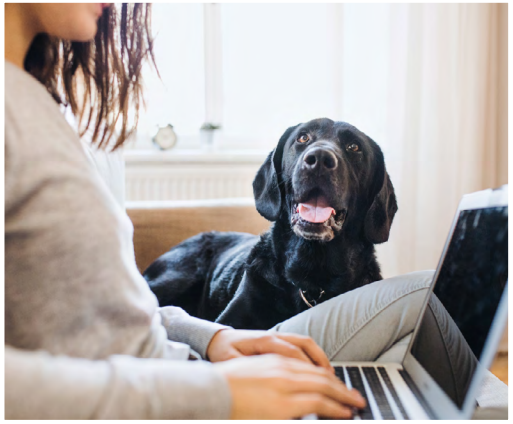
Inhalt

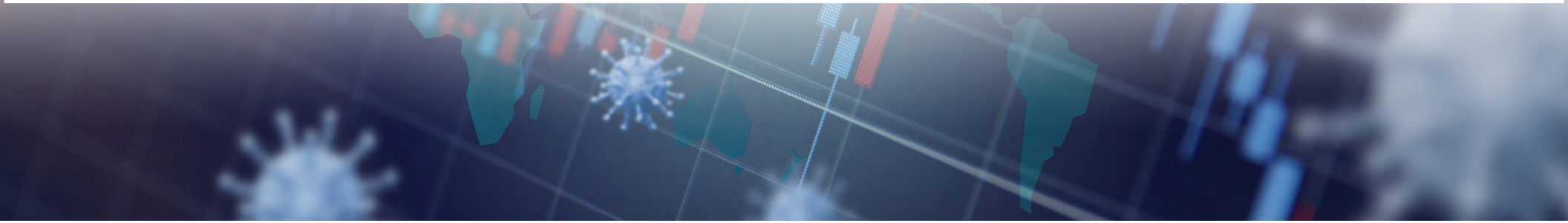
EINFÜHRUNG

Die Coronavirus-Pandemie hat die Unzulänglichkeiten der Geschäftskontinuität in vielen Unternehmen offengelegt und das langsame Tempo der Fortschritte bei der digitalen Transformation deutlich gemacht. Während sich der Staub legt, befinden sich viele Unternehmen in einer Phase intensiver Rationalisierung. Sie arbeiten daran, ihren Geschäftsbetrieb kurz- und mittelfristig fortzusetzen, und es fällt ihnen schwer, den weiteren Weg einzuschätzen. Dies ist umso schwieriger, als sie darüber nachdenken, wie sie ihre Mitarbeiter, Daten und Anwendungen über einen längeren Zeitraum - und vielleicht für immer - aus der Ferne sichern können.

Diese neue Realität macht eine Abkehr von einem traditionellen netzwerkzentrierten Sicherheitsmodell erforderlich, das davon ausgeht, dass jedem Gerät und Benutzer innerhalb des Netzwerks vertraut werden sollte. Da der Großteil der Endbenutzer nun remote arbeitet, hat sich die Einführung von Zero-Trust-Sicherheitsansätzen beschleunigt, insbesondere in Unternehmen. Wachsende Unternehmen, denen es häufig an internem Sicherheitsfachwissen mangelt, haben jedoch verständlicherweise Mühe, damit Schritt zu halten.

In diesem E-Book werden wir untersuchen, wie sich die Dynamik von COVID-19 auf die Sicherheit ausgewirkt hat. Wir erläutern die Bedeutung eines Zero-Trust-Ansatzes und erörtern, wie WatchGuard Ihrem Unternehmen helfen kann, die Sicherheit zu bieten, die Sie in diesen schwierigen Zeiten benötigen.





REMOTE-ARBEIT LÄSST SICHERHEITSBEDROHUNGEN IN DIE HÖHE SCHNELLEN

Bei allem, was sich durch COVID-19 geändert hat, sind einige Dinge gleich geblieben, da die Bedrohung für Unternehmen durch Cyberangriffe unvermindert anhält. Während sich einige Unternehmen auf den Modus „Überleben, um zu florieren" konzentrierten, nutzten Cyberkriminelle leider die Gelegenheit, Schwachstellen und bevorzugte Ziele zu identifizieren:

- Phishing-Angriffe haben massiv zugenommen, wobei täglich Dutzende von bösartigen Domänen auftauchten, die die Angst vor dem Coronavirus ausnutzen. Auf dem Höhepunkt der Krise meldete Microsoft allein in den USA täglich 70.000 Angriffe in Verbindung mit dem Thema COVID-19.[1] Viele dieser Kampagnen benutzten bekannte Phishing-Kits, die in diesen Zeiten schlicht umfunktioniert wurden.[2]

- Angesichts der explosionsartigen Zunahme gleichzeitig aktiver Benutzer auf Videokonferenzplattformen wie ZOOM – von 10 Millionen auf über 200 Millionen – warnte der CISA vor Versuchen böswilliger Cyber-Akteure, die zunehmende Nutzung beliebter Kommunikationsplattformen durch das Senden von Phishing-E-Mails, die bösartige Dateien enthalten, auszunutzen.[3]

- Alleine in den ersten vier Wochen der Krise stellten Sicherheitsforscher einen Anstieg um 41 Prozent bei der Anzahl der Geräte fest, die RDP dem Internet über den sehr anfälligen RDP-Standard-TCP-Port 3389 aussetzen.[4]

- Gefälschte Websites, die anscheinend legitime VPN-Clients anbieten und versprechen, Menschen zu schützen, verleiteten stattdessen Benutzer dazu, Malware herunterzuladen und auf ihren Rechnern zu installieren.[5]

- Ruchlose Nachbarn könnten die Tatsache ausnutzen, dass ihr Gebäude voll von Leuten ist, die von zu Hause aus arbeiten, wobei WLAN fast 50 Prozent des gesamten IP-Verkehrs ausmacht.[6]

1 https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
2 https://threatpost.com/covid-19-scam-scramble-cybercrooks-recycle/154383/
3 https://us-cert.cisa.gov/ncas/alerts/aa20-099a
4 https://www.bankinfosecurity.com/covid-19-driving-surge-in-unsafe-remote-connectivity-a-14035
5 https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
6 https://www.rehmann.com/resources-insights/business-wisdom-2/item/2740-it-leadership-8-remote-workforce-tips-for-optimal-access-security-and-productivity

ERWEITERUNG DES VPN-SCHUTZES REICHT NICHT

Die Nutzung von VPNs ist geradezu explodiert; innerhalb einer Woche beobachteten Forscher einen Traffic-Anstieg um 50 Prozent. Allein in den USA wurde ein Anstieg der VPN-Nutzung um 150 Prozent binnen eines Monats verzeichnet. Aufgrund der plötzlichen Umstellung der Anwender vom Büro aufs Homeoffice müssen nun viele Unternehmen ihren Mitarbeitern VPN-Lizenzen bereitstellen. Denn es besteht die Gefahr, dass Anwender ohne VPN-Verbindung gar nicht oder nur über unsichere Verbindungen auf benötigte Ressourcen zugreifen.

Die Benutzer brauchen nicht nur Sicherheit, wenn sie aus dem Netzwerk herausgenommen werden. Ebenso wichtig ist, dass über VPN-Verbindungen oder nach ihrer Rückverlagerung ins Büro keine Malware oder andere Bedrohungen eingeschleust werden, wenn sie wieder mit dem Firmennetzwerk verbunden werden. Während die Erweiterung des Netzwerkschutzes über VPN ein hohes Maß an Sicherheit bieten kann, erfordert die Art der heutigen Internetkriminalität mehr.

Wenn ein VPN isoliert verwendet wird, wird dem Endpoint ein übermäßiges Maß an Vertrauen entgegengebracht, was zur Verbreitung von Malware im weiteren Netzwerk führen kann. Unternehmen müssen begreifen, dass ihre Mitarbeiter jetzt de facto die erste Verteidigungslinie gegen Cyber-Bedrohungen sind.

Aus diesem Grund müssen IT-Teams damit beginnen, die Heimnetzwerke der Mitarbeiter so zu behandeln, als wären sie die digitale Version des Wilden Westens, denn:

- Es ist nur ein einziger gefährdeter Endpoint oder ein einziger gestohlener Berechtigungsnachweis erforderlich, um Ihre Umgebung zu infiltrieren.
- Fast zwei Drittel der Bedrohungen verbergen sich im verschlüsselten Datenverkehr.
- Einige Angriffe sind sehr zielgerichtet, andere wiederum betreffen zufällig entdeckte Ziele. Sie brauchen Schutz vor beiden.
- Die Nutzer stehen jetzt an vorderster Verteidigungslinie und müssen bei der Identifizierung, Vermeidung und Meldung von Bedrohungen unterstützt werden.

Die Nutzung von VPNs ist in die Höhe geschossen, mit einem **Traffic-Anstieg innerhalb einer Woche um 50 Prozent**. Allein in den USA wird mit einem **Anstieg der VPN-Nutzung um 150 Prozent binnen eines Monats gerechnet.**

EINSATZ VON ZERO-TRUST-NETZWERKEN

Verfügen Sie über einen Sicherheitssystem, das sich auf die Vermeidung von Datensicherheitsverletzungen durch die Beseitigung von ungerechtfertigtem Vertrauen konzentriert? Während ein traditionelles Netzwerk um die Idee des inhärenten Vertrauens herum aufgebaut ist, geht ein Zero-Trust-Rahmenwerk davon aus, dass jedes Gerät und jeder Benutzer, ob im Netzwerk oder nicht, ein Sicherheitsrisiko darstellt. Konzeptionell kann Zero-Trust als ein Sicherheitsansatz des „Niemals vertrauen, immer verifizieren" betrachtet werden. Er nutzt mehrere Schutzebenen zur Verhinderung von Bedrohungen, Blockierung von Lateral Movement sowie Durchsetzung nahtloser Benutzerzugriffskontrollen.

Das Zero-Trust-Framework basiert auf drei Grundsätzen:

1. Identifizierung von Benutzern und Geräten: Immer wissen, wer und was mit dem Unternehmensnetzwerk verbunden ist.

Während die Unternehmen damit zurechtkommen müssen, dass ihre Belegschaften nun vorwiegend remote arbeiten, ist die Sicherung des Zugangs zu internen Tools eine weitere große Herausforderung. Gleichzeitig nutzen Cyber-Kriminelle eine Vielzahl von Techniken, um Benutzernamen und Passwörter zu erlangen, wie Spear-Phishing, Social Engineering und den Kauf gestohlener Zugangsdaten im Dark Web. Ihr Ziel ist es, Zugang zum Netzwerk zu erhalten und dann wertvolle Firmen- und Kundendaten zu stehlen. Cloudbasierte Multifaktor-Authentifizierungsdienste (MFA) verringern das Risiko von Diebstahl von Benutzerdaten, Betrug und Phishing-Angriffen.

2. Bereitstellung eines sicheren Zugangs Beschränkung der Zugriffsberechtigungen von Geräten auf geschäftskritische Systeme und Anwendungen

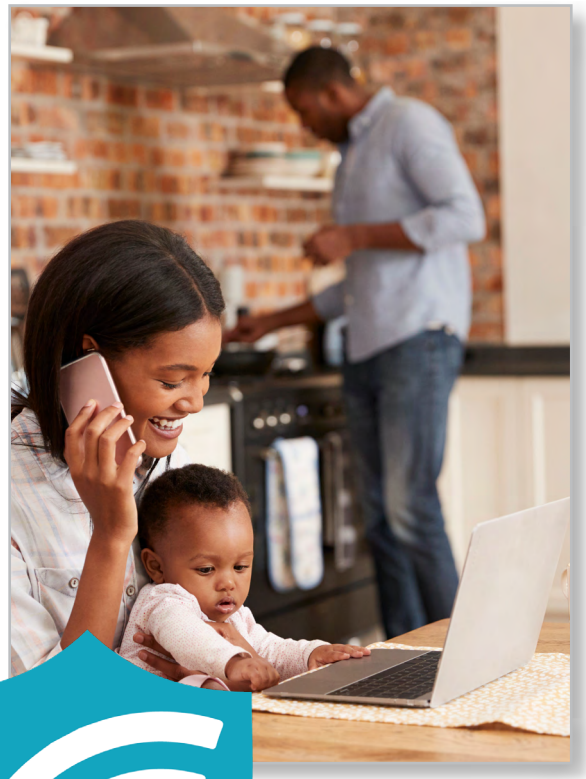
Im Rahmen des Zero-Trust-Konzepts besteht das Ziel der Zugriffsverwaltung darin, eine Möglichkeit zur zentralen Verwaltung des Zugriffs auf alle gängigen IT-Systeme bereitzustellen und gleichzeitig diesen Zugriff auf bestimmte Benutzer, Geräte oder Anwendungen zu beschränken. Entscheidungen über den Zugang sollten in Echtzeit auf der Grundlage der vom Unternehmen definierten Richtlinien und des Kontexts der Zugangsanfrage getroffen werden. Single-Sign-On-Technologien (SSO) in Kombination mit MFA können die Zugriffssicherheit verbessern und die Passwortbelastung für Benutzer minimieren.

3. Ständige Überwachung: Überwachung der Gesundheits- und Sicherheitslage des Netzwerks und aller verwalteten Endpoints.

Die Bedrohung durch Malware und Ransomware ist im Zuge des Coronavirus noch größer geworden. Auch das Risiko, sich mit solcher Schadsoftware zu infizieren, war noch nie höher, da im Homeoffice der Schutz durch die Firewall nicht mehr unbedingt gegeben ist. Und es ist schwieriger, die Sicherheit der Benutzer beim Navigieren im Internet zu gewährleisten, wenn sie sich von außerhalb Ihres Netzwerks verbinden.

Die Wahrscheinlichkeit, dass Homeoffice-Mitarbeiter ihre Unternehmens-Laptops das ein oder andere Mal für das private Surfen und Abrufen von E-Mails nutzen, ist ziemlich hoch. Um die Bedrohungen im Griff zu behalten, ist eine beständige, fortschrittliche Sicherheit erforderlich, die über den traditionellen Virenschutz hinausgeht.

EIN TRUSTED WIRELESS ENVIRONMENT AUFBAUEN



Beim Arbeiten in den eigenen vier Wänden kann es auch zu Sicherheitsbedenken im Zusammenhang mit dem WLAN kommen. Während Standorte auf der ganzen Welt, die aufgrund der COVID-19-Pandemie geschlossen wurden, ihre Wiedereröffnung in Erwägung ziehen, bereiten sich die Netzwerkadministratoren darauf vor, bei der Rückkehr der Mitarbeiter ins Büro auf Hochtouren zu arbeiten. Wer weiß, welche Ransomware sie bei der Nutzung des WLAN zuhause möglicherweise auf ihren Firmenlaptops eingefangen haben?

Mit einem Trusted Wireless Environment können Sie:

- Erkennung und Ursachenanalyse von Fehlern und Anomalien automatisieren.
- In Echtzeit erkennen, wenn die Verbindungsherstellung bei WLAN-Clients fehlschlägt, und die Ursache identifizieren (das heißt, ob das Problem mit dem WLAN, Netzwerkdienst oder einem Client-Gerät und/oder einer Client-Anwendung zusammenhängt).
- Standardmäßige Bilddateien für Etagengrundrisse ganz einfach für jeden Standort importieren. Nach dem Hinzufügen können Sie per Rechtsklick auf alle Verwaltungs- und Fehlerbehebungsfunktionen für jeden Access Point zugreifen. Heatmaps zeigen die Zugriffspunktabdeckung, die Verbindungsgeschwindigkeit und die Kanalabdeckung.

Rückkehr ins Büro? WLAN kann beim Einhalten der Abstandsregeln helfen

Fördern Sie eine sichere Arbeitsumgebung mit automatisierter Überwachung der Einhaltung von Abstandsregeln durch WLAN-Cloud-Management. WLAN-Zugangspunkte können Echtzeit-Messungen des Personenaufkommens, Warnungen und Benachrichtigungen liefern, wenn sich Kapazitätsgrenzen nähern oder überschritten werden.

Mit dem WLAN-basierten Crowd-Monitoring können Unternehmen:

- Mitarbeiterversammlungen und Sitzungsabläufe verwalten
- Ankommende und abreisende Besucher, einschließlich Bewegungen, analysieren
- Einhaltung von Gesundheits- und Menschenmengenbeschränkungen nachweisen
- Bewertungen von Geschäftsabläufen, Planung, wirtschaftlichen Auswirkungen und Vermögen mit verwertbaren Daten verbessern
- Komplett anonym; Datenschutz- und DSGVO-konform

WATCHGUARD SICHERHEIT ZERO-TRUST-LEITFADEN

Die Anwendung einer Zero-Trust-Strategie kann Ihrem Unternehmen helfen, einen moderneren Ansatz für die Cybersicherheit zu entwickeln. Die gute Nachricht ist, Sie brauchen sich nicht alleine darum zu kümmern. Unabhängig davon, ob Ihre IT-Abteilung zu klein ist oder ob Sie überhaupt kein IT-Personal haben: Managed Service Provider bieten die Leistung, die Unternehmen benötigen, um sich auf eine robuste Infrastruktur verlassen zu können. Diese ermöglicht es mobilen Benutzern, von jedem Gerät und überall zu arbeiten und Zugang zu öffentlichen Cloud-Diensten zu erhalten und gleichzeitig die Sicherheit des Unternehmens zu gewährleisten.

WatchGuard liefert Zero-Trust-Sicherheit

1. Benutzeridentitäts- und Geräteschutz, der sich besonders für Zero-Trust-Umgebungen eignet:

- **100 % cloudverwaltet.** Mit WatchGuard Cloud können Sie Ihre Sicherheit verwalten und Berichte über Ihre Sicherheit von nur einer leistungsstarken Plattform aus erstellen. Unabhängig davon, ob Sie die Infrastrukturkosten reduzieren oder eliminieren, die Einrichtung beschleunigen, entfernte Standorte in beliebigem Umfang einrichten, Ihre Sicherheitsmanagement-Tools vereinfachen oder einen besseren Einblick in Ihr Netzwerk erhalten möchten, WatchGuard Cloud kann Ihnen helfen.
- **DNA des Mobilgeräts.** Clevere Bedrohungsakteure haben gezeigt, dass sie in der Lage sind, mobile Geräte zu klonen und das neue, nachgeahmte Telefon zur Authentifizierung in Systemen zu nutzen, um die MFA zu durchbrechen. WatchGuards einzigartige Funktion DNA des Mobilgeräts nimmt einen Fingerabdruck der Merkmale, die für jedes mobile Gerät einzigartig sind. Bei jedem Einloggen eines Benutzers wird die AuthPoint App diese DNA des Mobilgeräts neu erstellen und in eine Berechnung des Einmalpassworts (OTP) einbeziehen, um sicherzustellen, dass nur das Originalgerät die Authentifizierung durchführen kann.
- **Integration Dritter.** Das Ökosystem von WatchGuard umfasst Dutzende von Drittanbieter-Integrationen mit AuthPoint. So können Unternehmen verlangen, dass Benutzer den Authentifizierungsprozess durchlaufen, bevor sie auf sensible Cloud-Anwendungen, VPNs 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.

2. Vereinfachter sicherer Zugang an allen Fronten:

- **AuthPoint-Integration mit führenden IAM-Plattformen.** Unternehmen setzen Identitäts- und Zugriffsmanagement-Lösungen ein, um den Benutzern die vollständige Kontrolle und einen einfachen Zugriff über alle Anwendungen ihres Unternehmens hinweg zu ermöglichen. WatchGuard AuthPoint integriert sich direkt mit den führenden IAM-Plattformen auf dem Markt, darunter CyberArk, Akamai, Oracle, und andere.
- **WatchGuard Firebox und Access Portal.** Access Portal ist eine clientlose VPN-Lösung, die standardmäßig mit jeder Firebox geliefert wird und sicheren Fernzugriff für Remote-Benutzer bietet. Mit Access Portal benötigen Benutzer lediglich einen Webbrowser, um eine Verbindung zu Webanwendungen von Drittanbietern, internen Anwendungen und Microsoft Exchange-Diensten herzustellen sowie RDP- und SSH-Sitzungen zu lokalen Ressourcen zu erstellen.
- **Sichere VPN Enforcement und Host Isolation**. Unsere einzigartige Threat Detection and Response (TDR)-Plattform vereinigt Netzwerksicherheits- und Endpoint-Sicherheitsfunktionen, um zu verhindern, dass potenziell infizierte Computer Malware in das breitere Netzwerk einschleusen. Mit TDR können Sie einen aktiven Host-Sensor auf jedem Gerät anfordern, das versucht, direkt oder über VPN eine Verbindung zum Netzwerk herzustellen. Außerdem überwacht der Host-Sensor den Zustand des Geräts aktiv und isoliert es, wenn es zu einem Risiko wird.

3. Netzwerke, Endpoints und Benutzer sind sicher, unabhängig davon, wo sich Menschen verbinden:

- **DNS-Filterung mit DNSWatch und DNSWatchGO.** Mit Cloud-basierter DNS-Filterung können bestimmte Verbindungen gesperrt und der Zugang zu riskanten Bereichen des Internets eingeschränkt werden, ohne den Datenverkehr zurück durch Ihr Netzwerk zu leiten. Klicks auf bösartige Links oder Versuche, sich mit Domains zu verbinden, die mit Phishing und Malware in Zusammenhang gebracht werden, werden automatisch gesperrt.
- **AD360 Endpoint Detection and Response.** Das Abfangen ausgefeilter Malware erfordert ebenso ausgefeilte Methoden. AD360 vereint mehrere Erkennungsmethoden, etwa Verhaltens-, heuristische und Sandbox-Analysen, auf einer einzigen Plattform. Die KI-Fähigkeiten von AD360 ermöglichen es, Bedrohungen vorherzusehen und automatisch zu blockieren, bevor der Schaden einsetzt, sowie Anomalien aufzudecken, die ein menschlicher Analytiker übersehen könnte.
- **WatchGuard Firebox und die Total Security.** Als Herzstück des Netzwerks bietet eine WatchGuard Firebox mehrschichtige Sicherheit auf Enterprise-Niveau, die die neuesten Bedrohungen abwehrt.
- **Threat Detection and Response.** Mit TDR integriert WatchGuard Endpoint- und Netzwerk-Telemetrie in der Cloud und korreliert Sicherheitsdaten, um Bedrohungen zu erkennen und auf sie zu reagieren, die sonst in der Isolation übersehen würden.
- **Automation Core.** Die Lösungen von WatchGuard sind in hohem Maße automatisiert, so dass sie Zyklen für manuelle und wiederholbare Prozesse einsparen können. Die Automatisierung rationalisiert alles, von Antiviren-Updates und Patch-Management bis hin zur Erkennung von Anomalien und Warnmeldungen. Darüber lassen sich Sicherheitsprozesse nahtlos mit Professional Services Automation (PSA)-Tools integrieren. Zudem können Sie dank der engen Integration von Remote Monitoring and Management(RMM)-Tools schneller auf Supportanfragen eingehen.

BEGINNEN SIE MIT DER PLANUNG VON ZERO-TRUST FÜR IHRE GESCHÄFTE

Die gegen die Ausbreitung des neuartigen Virus ergriffenen Maßnahmen sind beispiellos, und das darunter fallende „Experiment Heimarbeit" ist für viele Unternehmen vollkommen unbekanntes Terrain. Da der Großteil der Endbenutzer heute remote arbeitet, können Null-Trust-Sicherheitsansätze dazu beitragen, Kontinuität und Sicherheit aufrechtzuerhalten.

Managed Service Provider können eine entscheidende Rolle dabei spielen, Ihrem Unternehmen die erforderlichen Fähigkeiten und Ressourcen zur Verfügung zu stellen, um Zero-Trust-Netzwerke effektiv einzusetzen. Die Auslagerung der Verantwortung an einen Lösungsanbieter sorgt dafür, dass Sie sich absolut sicher und gelassen fühlen können. Sie können sich also ganz auf das Wachstum Ihres Unternehmens konzentrieren, um in Ihrem Bereich wettbewerbsfähig bleiben.

Weitere Informationen über WatchGuard Partner und ihr Produktangebot finden Sie unter https://watchguardsupport.secure.force.com/PartnerFinder/.

„Dank WatchGuard und unserem MSP, Calvert Technologies, sind wir jetzt gelassen, wenn es um unsere IT-Sicherheit geht. Anstatt uns über das Risiko Sorgen machen zu müssen, Opfer eines Cyberangriffs oder einer Datensicherheitsverletzung zu werden, können wir uns darauf konzentrieren, unseren Kunden den bestmöglichen Service zu bieten."

- Carson Coz, IT-Manager, Mykra

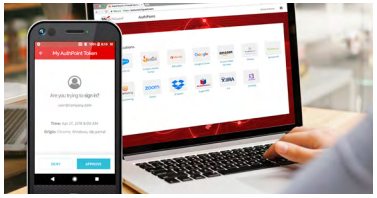
WatchGuard Unified Security Platform™

Network Security

Network-Security-Llösungen 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 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.



Multifaktor-Authentifizierung

Mit WatchGuard AuthPoint® können Sie die passwortgestützte Sicherheitslücken 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 Cloud-natives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung Panda Adaptive Defense 360 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.

Vertrieb Nordamerika: 1.800.734.9905 • Vertrieb in Deutschland, Österreich und der Schweiz: +49 700 92229333 • Web: www.watchguard.de