NETZWERKSICHERHEIT FÜR DEZENTRALE PRODUKTIONSUNTERNEHMEN

WatchGuard®

INHALTSVERZEICHNIS

NETZWERKSICHERHEIT IN DER PRODUKTIONSHALLE DANK WATCHGUARD

Fertigungsbetriebe sind nach dem Gesundheitswesen eine der am häufigsten gehackten Branchen der Welt.[1] Während Hersteller ihre Produktionsstätten modernisieren und hochentwickelte Betriebstechnologienetzwerke (Operational Technology, OT) einrichten, werden sie zunehmend zur Zielscheibe für Cyberkriminelle. Seit 2018 haben Angriffe auf OT-Netzwerke um 2.000 %[2] zugenommen. Dabei haben 47 %[3] der Datenlecks bei Produktionsunternehmen zum Verlust von geistigem Eigentum geführt. Die Cybersecurity Infrastructure and Security Agency hat vor Kurzem eine Warnung vor eskalierenden Angriffen auf OT-Netzwerke veröffentlicht, insbesondere Spear Phishing- und Ransomware-Angriffe auf minimal geschützte Umgebungen.

2.000 %
mehr Angriffe auf OT-Netzwerke

47 %
der Datenlecks bei Produktionsunternehmen haben zum Verlust von geistigem Eigentum geführt

Produktionsunternehmen wissen, dass eine Störung ihrer Betriebssysteme zu einem kompletten Produktionsausfall führen kann, sind sich aber nicht unbedingt der Sicherheitsauswirkungen eines ungeschützten Netzwerks bewusst. In diesem E-Book werden die einzigartigen Sicherheitsherausforderungen für dezentrale Produktionsunternehmen vorgestellt und Tipps für die Sicherung von OT-Netzwerken gegeben.

[1] Precision Manufacturing
[2] https://www.tripwire.com/state-of-security/security-data-protection/attacks-targeting-assets-grew-report-reveals/
[3] 2018 Data Breach Investigation Report (Bericht zu Datensicherheitsverletzungen 2018) von Verizon

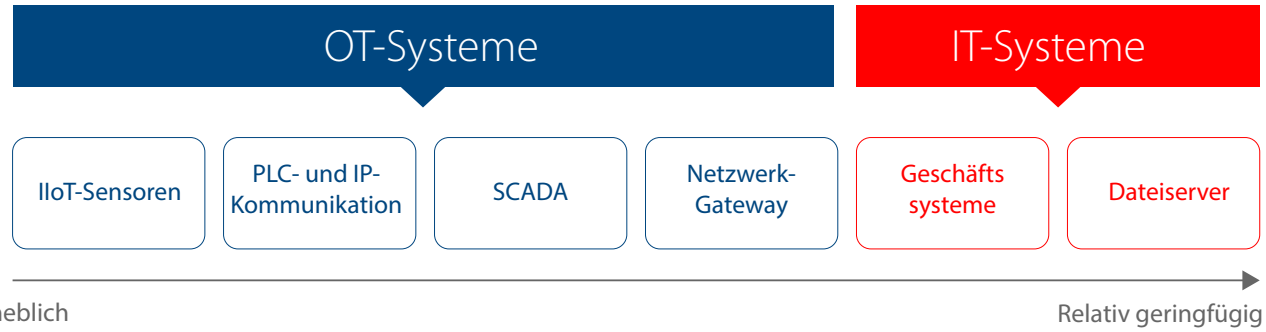
WAS IST BETRIEBSTECHNOLOGIE?

Gartner definiert Betriebstechnologie (Operational Technology) als „… Hardware und Software, die durch direkte Überwachung und/oder Steuerung von Industriegeräten, Anlagen, Prozessen und Ereignissen Änderungen erkennen oder verursachen.“[4] OT-Netzwerke umfassen in der Regel alle vernetzten Geräte aus der Fertigungshalle sowie die KI-, Robotik- und Kontrollsysteme, von denen diese abhängig sind. Diese Technologien sind für moderne Produktionsunternehmen unerlässlich, bringen aber wesentliche Sicherheitsschwachstellen in zuvor sicheren Umgebungen mit sich.

Herausforderungen bei der Sicherung von OT-Umgebungen:

- ✖ OT-Netzwerke verwenden Altgeräte, oft mit **veralteten Betriebssystemen**, die sich nur schwer für die Abwehr der neuesten Bedrohungen aktualisieren lassen.
- ✖ Aufgrund der Anforderungen hinsichtlich Hochverfügbarkeit und **Produktionsplänen** kann die Produktion nicht einfach unterbrochen werden, wenn Updates erforderlich sind.
- ✖ Systeme werden in der Regel nur aktualisiert oder ersetzt, wenn sie **unbrauchbar werden**.
- ✖ Geringfügige Änderungen an der OT-Umgebung können sich **erheblich auf den ganzen Betrieb auswirken**.

Auswirkungen von Ausfallzeiten auf Hersteller



[4] https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

HERAUSFORDERUNGEN IN DER CYBERSICHERHEIT FÜR PRODUKTIONSUNTERNEHMEN

Innovative neue IIoT-Technologien (Industrial Internet of Things) wie Konstruktionsrobotik und intelligente Fertigungsstraßen ermöglichen einerseits den Herstellern optimierte Betriebsabläufe und einen Wettbewerbsvorteil, setzen sie aber andererseits auch Risiken durch Hacker aus.

Wesentliche Herausforderungen:

- **Diebstahl von geistigem Eigentum.** Der Diebstahl geistigen Eigentums ist ein seit Langem bestehendes Problem im Produktionssektor und kann alles von Produktideen bis hin zu patentierten Fertigungsprozessen zum Ziel haben. All das stellt eine verlockende Beute für Wettbewerber und Hacker dar, die Ransomware einsetzen. Angriffe dieser Art können zum Verlust von Umsätzen und Kunden führen.
- **Mangel an Fachkräften für die Cybersicherheit.** Ein weltweiter Mangel an IT-Fachkräften sorgt in allen Branchen für große Personalsorgen, ist aber besonders für den Produktionssektor ein Problem, da diese Branche sich mehr als andere auf eine eigene digitale Infrastruktur (Betriebstechnologie und industrielle Kontrollsysteme (Industrial Control Systems, ICS) stützt. Hierdurch sinkt die Zahl geeigneter Bewerber noch weiter.
- **Schatten-IT.** Die Nutzung von Hardware oder Software in einem Unternehmen ohne Wissen der IT-Abteilung entwickelt sich zunehmend zu einem Problem für viele Produktionsunternehmen, da Betriebsteams ohne das Wissen einer zentralen IT-Abteilung vernetzte Geräte kaufen und einsetzen.
- **Extreme Betriebsbedingungen.** Fertigungshallen sind selten sauber und steril, sondern meist heiß und staubig. Einige Hersteller müssen das WLAN sogar auf Außenbereiche ausweiten, wo sie der Witterung ausgesetzt sind. Diese Bedingungen können zu einem schnelleren Ausfall von Netzwerkgeräten führen, wodurch das Risiko von Ausfallzeiten größer wird.

NSA UND CISA WARNEN VOR ANGRIFFEN AUF OT-NETZWERKE

Der plötzliche Wechsel zu Remotearbeit aufgrund von COVID-19 hat eine beschleunigte Angriffsrate auf OT-Netzwerke zur Folge. Daher haben NSA und CISA nun Warnungen ausgesprochen. Diese besagt: „Veraltete OT-Assets, die nicht für den Schutz vor böswilligen Cyberaktivitäten konzipiert sind, führen zusammen mit den einfach abrufbaren Informationen zur Identifizierung von OT-Assets, die über das Internet verbunden sind, zu einer äußerst kritischen Lage ...“[5]

Zuletzt angewendete Taktiken, Techniken und Prozesse:

- **Spear Phishing** zum Erlangen des anfänglichen Zugriffs auf das IT-Netzwerk des Unternehmens vor dem Eindringen in das OT-Netzwerk.
- Bereitstellung von **im Handel erhältlicher Ransomware** zum Verschlüsseln von Daten in beiden Netzwerken.
- Verbindung mit **über das Internet zugänglichen SPS, die keine Authentifizierung** für den anfänglichen Zugriff erfordern.
- Nutzung von **häufig verwendeten Ports und Standard-Anwendungsschichtprotokollen** für die Kommunikation mit Controllern und das Herunterladen geänderter Steuerungslogik.
- Nutzung der **Engineering-Software von Anbietern** und **Programmdownloads**.
- Änderung von Steuerungslogik und -parametern auf SPS.

Auswirkung:

Verfügbarkeitsausfall des OT-Netzwerks.	Weniger Transparenz für menschliche Bediener.	Verminderung von Produktivität und Umsatz.	Schädliche Manipulation der Steuerung und Störung physischer Prozesse.

[5] https://us-cert.cisa.gov/ncas/alerts/aa20-205a

FALLSTUDIE: HERSTELLER VON BEATMUNGSGERÄTEN FÄLLT RANSOMWARE ZUM OPFER

Im Zuge der COVID-19-Pandemie erklärte sich ein Hersteller von Verkehrskommunikationssystemen in Long Island, New York, bereit, Beatmungsgeräte zu produzieren. Dabei war sich das Unternehmen nicht bewusst, dass es durch diese Arbeit zum Wohle der Gemeinschaft zu einer Zielscheibe für eine führende Ransomware-Gruppe werden würde. Nach einem DopplePaymer-Ransomware-Angriff kam die Produktion dieses Herstellers, der fast 300 behördlich zugelassene Beatmungsgeräte produziert hatte, zum Stillstand.

Profil des Opfers

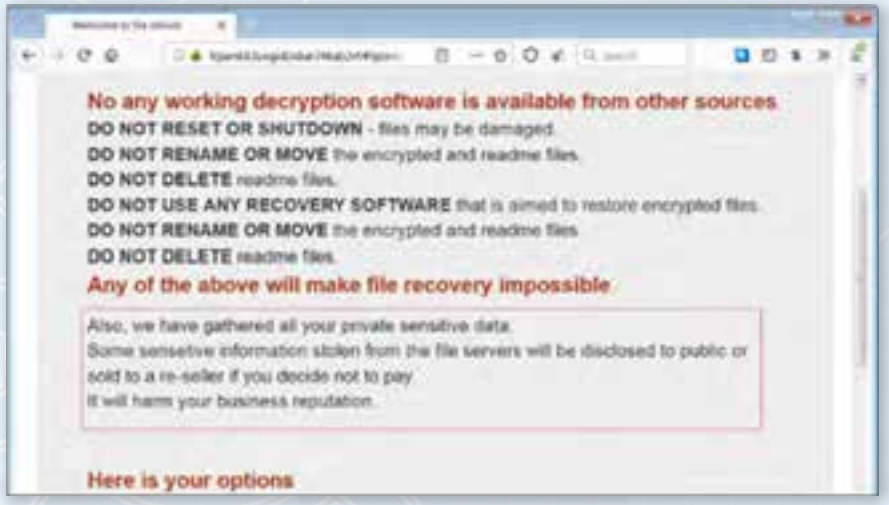
- Anzahl Mitarbeiter: ~ 110
- Umsatz: Weniger als 25 Millionen US-Dollar jährlich

Ziel/Methode des Angreifers

- Einführung von Ransomware über Phishing-E-Mails
- Blockierung der Produktionsstätte
- Forderung eines Lösegelds für die Rückgabe der Daten und damit diese nicht öffentlich verbreitet werden (Daten wurden nicht nur verschlüsselt, sondern auch extrahiert/kopiert)

Tools

- **DopplePaymer-Ransomware**: Diese Ransomware-Variante wurde im Frühsommer 2019 entdeckt. Dabei werden Anwender zur Zahlung eines Lösegelds in Höhe von 2 bis 100 Bitcoins (BTC) bzw. 20.000 bis 100.000 US-Dollar aufgefordert.



Die Tor-Zahlungssite von DoppelPayment für die Lösegeldzahlung von BleepingComputer

1 SICHERHEITSANALYSE AUTOMATISIEREN, UM BEDROHUNGEN SCHNELL ZU ERKENNEN UND DARAUF ZU REAGIEREN

Sie benötigen einen hohen Grad Automatisierungsgrad, um mit Bedrohungen Schritt zu halten, Zeit- und Geldverschwendung zu reduzieren sowie die Transparenz einer modernen Netzwerkumgebung zu erhöhen. Ausfallzeiten und Produktionsunterbrechungen können schwerwiegende Folgen für einen Hersteller haben und seinen Ruf bei den Kunden zerstören. Ransomware und Cryptomining-Malware können die Produktion zum Stillstand bringen, die Effizienz senken und die Betriebskosten erhöhen. Mit Automatisierung können Sie die Erkennung und Reaktion beschleunigen und sicherstellen, dass Systeme von Anfang an richtig konfiguriert werden.

Einheitliche Sicherheitsplattformen sind von Grund auf mit Automatisierung konzipiert und können die Sicherheit Ihres Netzwerks nicht nur aufrechterhalten, sondern auch über den traditionellen Perimeter hinaus erweitern. Fertigungsumgebungen mit Automatisierung decken alle vier Automatisierungsebenen ab (Verwaltung, betrieblich, reaktionsschnell und vorausschauend) und können die neuesten Bedrohungen für Produktionsunternehmen abwehren.

Achten Sie auf:

- Reaktionsschnelle Automatisierungsfunktionen, die VPN-Verbindungen zu infizierten Geräten blockieren und Infektionen beheben.
- KI-gestützten vorausschauenden Schutz, um die komplexen Bedrohungen abzuwehren, die ansonsten ein Expertenteam erfordern würden.
- Integration in RMM- und PSA-Tools für schnellere Supportreaktionen.

2 PHISHING-VERSUCHE MIT DNS-FILTERUNG ABWEHREN

Das Phishing ist die einfachste Möglichkeit für einen Hacker, in ein Netzwerk einzudringen. Produktionsunternehmen sind derzeit ganz besonders von dieser Art von Angriff betroffen. Tatsächlich wurde Spear Phishing 2018 bei 71 % der Angriffe auf Produktionsunternehmen genutzt.[6] Im gleichen Zeitraum hat im Schnitt einer von 41 Fertigungsmitarbeitern eine Phishing-E-Mail erhalten.

Spear Phishing wurde 2018 bei
71 %
aller Angriffe auf Produktionsunternehmen genutzt

Sie können Ihr Unternehmen schützen, indem Sie böswillige E-Mails von Mitarbeitern fernhalten und riskante Klicks blockieren. Hacker täuschen ahnungslose Opfer per DNS. Eine genaue Untersuchung von DNS-Anforderungen trägt also enorm dazu bei, Angriffe zu erkennen und letztendlich abzuwehren. Wenn Anwender unwissentlich auf schädliche DNS-Adressen zugreifen, können diese Zugriffe automatisch blockiert werden. Dabei werden Anwender nahtlos zu einer sicheren Landingpage umgeleitet.

Achten Sie auf:

- Lösungen, die bösartige Clickjacking- und Phishing-Domains unabhängig von Verbindungstyp, Protokoll oder Port blockieren.
- Die Fähigkeit, sowohl Phishing-Versuche als auch Command-and-Control-Kanäle zu blockieren.
- Angebote, die Anwender, die einem Phishing-Versuch zum Opfer fallen, in Echtzeit informieren.

[6] Proofpoint Human Factor Report, 2018

3 VERSCHLÜSSELTEN DATENVERKEHR ANALYSIEREN

Mehr als 80 %[7] des geschäftlichen Datenverkehrs findet über verschlüsselte Kanäle statt, und 50 %[8] der Phishing-Sites verbergen ihre Angriffe mit HTTPS. Bei vielen erfolgreichen Cyberangriffen werden bekannte Malware-Payloads einfach wiederverwendet, aber in verschlüsseltem Datenverkehr verborgen, bis es zu spät ist. Die Transparenz dieses Datenverkehrs ist entscheidend. Wenn Sie HTTPS-Entschlüsselung und Inhaltsanalyse nicht nutzen, entgehen Ihnen wahrscheinlich zwei Drittel[9] der Malware, die in Ihr Unternehmen eindringt.

Durch die HTTPS-Analyse können Sie HTTPS-Datenverkehr entschlüsseln, den Inhalt auf Angriffshinweise überprüfen und ihn dann wieder mit einem neuen Zertifikat für eine sichere Übermittlung verschlüsseln.

Mehr als 80 %
des geschäftlichen Datenverkehrs findet über verschlüsselte Kanäle statt

50 %
der Phishing-Sites verbergen ihre Angriffe mit HTTPS

Achten Sie auf:

- Eine Firewall mit leistungsstarker HTTPS-Analyse, wenn ALLE Sicherheitsdienste aktiv sind.
- Eine Lösung, die eine VOLLSTÄNDIGE Analyse von TLS 1.3 unterstützt.

[7] https://www.gartner.com/imagesrv/media-products/pdf/radware/Radware-1-2Y7FR0I.pdf
[8] https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/
[9] https://watchguard.widen.net/view/pdf/zibigxjggd/WG_Threat_Report_Q1_2020.pdf

4 MEHRSTUFIGE SICHERHEIT UND SCHUTZ VOR ZERO-DAY-ANGRIFFEN IMPLEMENTIEREN

Die Vernetzung von Remote-Standorten und industriellen Umgebungen kann zwar die betriebliche Effizienz steigern, die Auswirkungen auf die Sicherheit können jedoch gravierend sein. Verstöße gegen industrielle Kontrollsysteme (Industrial Control Systems, ICS) können erhebliche Auswirkungen haben, die Ihr Unternehmen zum Stillstand bringen und sogar potenziell lebensbedrohlich sein können. Dezentrale Produktionsunternehmen müssen in der Lage sein, OT-/IOT-Netzwerke von IT-Ressourcen zu trennen und dabei den gesamten Netzwerkverkehr auf Bedrohungen zu untersuchen. SCADA-spezifische IPS-Signaturen können Schutz vor bekannten Exploits gängiger industrieller Kontrollsysteme bieten. Außerdem können moderne Anti-Malware-Ansätze wie Sandboxing und KI-gestützte Abwehr Ihr Unternehmen vor Zero-Day-Angriffen schützen.

Achten Sie auf:

- KI-gestützte Lösungen zum Schutz vor Malware, die auch Stellen abdecken, an denen reguläre Signaturaktualisierungen schwierig sind.
- SCADA/SPS-spezifische Signaturen, die vor gängigen Bedrohungen in der Fertigungsbranche schützen.

5 SICHEREN ZUGRIFF ERWEITERN

Produktionsunternehmen nutzen ein dezentrales Ökosystem von Mitarbeitern, Partnern, Auftragnehmern und Lieferanten, die allesamt unterschiedliche Zugriffsebenen für die Unternehmensanwendungen benötigen. Mit Single Sign-On können Anwender sich mit einem Satz Anmeldedaten einmalig anmelden, um auf alle Anwendungen, Websites und Daten, die sie brauchen, zuzugreifen. SSO verbessert die Sicherheit, da Anwender sich weniger Passwörter merken müssen, und entlastet die IT-Teams, bei denen ansonsten zahlreiche Anfragen für Passwortrücksetzungen eingehen. Kombinieren Sie SSO mit Multifaktor-Authentifizierung (MFA), um RDP-(Remotedesktop-), SSH- und Webzugriffsverbindungen zu sichern. Diese Best Practice kann verhindern, dass Remoteverbindungen als Trojaner in Ihr Netzwerk dienen.

Achten Sie auf:

- SSO, das die gängigen Identitätsanbieter unterstützt, wie AuthPoint, Shibboleth, OneLogin, ADFS und Okta.
- Eine Lösung, die die gängigsten Softwaretoken unterstützt, darunter AuthPoint, Okta Mobile, Google Authenticator, OneLogin Protect, Duo Mobile, RSA SecureID.

6 TRUSTED WIRELESS ENVIRONMENT AUFBAUEN

Während immer mehr Geräte in der Fertigungshalle per WLAN vernetzt werden, sollten Sie unbedingt eine Trusted Wireless Environment implementieren, um diese Geräte vor Kompromittierung zu schützen. Eine Trusted Wireless Environment ist ein Konzept für den Aufbau eines WLAN, das schnell, leicht zu verwalten und vor allem sicher ist.

Eine Trusted Wireless Environment bietet automatischen Schutz vor den sechs bekannten Kategorien von WLAN-Bedrohungen:

1. Rogue Access Points
2. Rogue-Clients
3. Benachbarte Access Points
4. Ad-hoc-Verbindungen
5. Evil Twin Access Points
6. Fehlerhaft konfigurierte Access Points

Achten Sie auf:

- Wireless Intrusion Prevention (WIPS), das automatisch vor den sechs bekannten Kategorien von WLAN-Bedrohungen schützt und gleichzeitig den Betrieb legitimer externer Access Points in derselben Umgebung zulässt.
- WLAN, das verhindert, dass Anwender eine Verbindung zu nicht zugelassenen WLAN Access Points herstellen, aber nicht die legitimen Access Points in der Nähe beeinträchtigt.

7 ROBUSTE SICHERHEIT FÜR EXTREME BEDINGUNGEN VERWENDEN

Die meisten Netzwerkgeräte sind für Büroumgebungen oder die Rack-Montage in einem klimatisierten Serverraum ausgelegt, in dem Probleme durch Temperatur, Wasser und Staub vernachlässigbar sind. Initiativen zur Vernetzung und Modernisierung von Betriebsabläufen unter extremen Umgebungsbedingungen erfordern ein Gerät, das diesen Bedingungen standhalten kann, effektive Sicherheit bietet und eine gleichbleibend hohe Leistung erbringt. Staub, Feuchtigkeit und extreme Temperaturen können die Lebensdauer und Leistung von Netzwerk-Hardware erheblich verringern.

Robuste Netzwerksicherheitsprodukte haben eine IP-(Ingress Protection-)Bewertung für Widerstand gegen feste Körper (0–6) und Flüssigkeiten (0–8) und bieten somit angemessenen Schutz für Ihre Umgebung.

Achten Sie auf:

- Lösungen mit IP-Bewertung IP64 und höher.
- Robuste WLAN-Access Points für die Verlagerung von Geräten in Außenbereiche.

	Schutz vor festen Objekten		Schutz vor Flüssigkeiten
Erste Zahl	Beschreibung	Zweite Zahl	Beschreibung
0	Kein Schutz	0	Schutz
1	Schutz vor festen Objekten über 50 mm (z. B. Hände)	1	Schutz vor vertikal fallenden Wassertropfen
2	Schutz vor festen Objekten über 12 mm (z. B. Finger)	2	Schutz vor direktem Spritzwasser bis zu 15 Grad
3	Schutz vor festen Objekten über 2,5 mm (z. B. Werkzeuge)	3	Schutz vor direktem Spritzwasser bis zu 80 Grad
4	Schutz vor festen Objekten über 1 mm (z. B. Drähte)	4	Schutz vor direktem Spritzwasser von allen Richtungen
5	Komplettschutz vor Staub	5	Schutz vor Wasser mit niedrigem Druck aus allen Richtungen
		6	Komplettschutz vor starken Wasserstrahlen
		7	Schutz bei Eintauchen bis zu einer Tiefe von 1 m
		8	Schutz bei Eintauchen unter Druck

*„WatchGuard erzielte eine **hohe Sicherheitseffektivität** und **niedrige Gesamtbetriebskosten** und ist **eines von nur zwei Produkten, die 100 % der Ausweichmanöver blockierten**."*

- NSS Labs

Firebox T35-R
IP64-konformes Industriegehäuse, das sowohl staub- als auch spritzwassergeschützt ist.

AP327X
IP64-Bewertung für die extremsten Umgebungen.

Weitere Informationen finden Sie unter WatchGuard.com/Manufacturing.

WATCHGUARD UNIFIED SECURITY PLATFORM™

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 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 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 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.

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 Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 250.000 Kunden zu schützen. 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.

Weitere Informationen finden Sie unter WatchGuard.de.

Vertrieb Nordamerika: +1 800 734 9905 • Vertrieb: +49 700 9222 9333 • www.watchguard.com/de