Es geht auch

einfacher

– in vier Schritten zu mehr Sicherheit

WatchGuard®

Inhaltsverzeichnis

Einführung

Die Komplexität und Ausgereiftheit von Cyberbedrohungen nimmt immer mehr zu und zwingt somit Unternehmen, leistungsstärkere und umfassendere Abwehrmechanismen zu suchen. Doch was ist das größte Problem bei der Erweiterung der Sicherheitsmaßnahmen, um diesen komplexeren Anforderungen gerecht zu werden? Ihre Ressourcen. Denn die Zeit und Zahl der Mitarbeiter, die Sie für diese Aufgaben zur Verfügung stellen können, bleibt unverändert.

Ein voller Werkzeugkasten bringt nicht viel, wenn es niemanden gibt, der den Hammer schwingt. Und auch Sicherheitsinfrastrukturen verwalten sich nicht von selbst. Branchenweit herrscht jedoch in vielen IT-Abteilungen Personalmangel und dieser Trend scheint kein Ende zu nehmen. **Unglaubliche 53 % der weltweit befragten IT-Profis gaben an, dass die Zahl der Mitarbeiter mit Kompetenz im Bereich Cybersicherheit in ihrem Unternehmen alarmierend niedrig ist**[1]**.** Generell sind die Abteilungen dünn besetzt. Für die Mitarbeiter bedeutet das, dass sie nicht nur ihre alltäglichen Aufgaben erfüllen, sondern gleichzeitig auch Warnhinweisen nachgehen und Support-Tickets bearbeiten müssen.

Wenn Sie dieses Szenario aus Ihrem Unternehmen kennen und es Ihnen schier unmöglich erscheint, die Verwaltung der Cybersicherheit zu vereinfachen, werden Sie die vier nachfolgend vorgestellten Maßnahmen interessieren.

Kompliziert

Management ungleichartiger Einzellösungen:

Sie kommen Montagmorgen ins Büro und erhalten ein Support-Ticket von einem Kollegen aus der Marketing-Abteilung. Darin steht: „Kein Zugriff auf ein wichtiges Dokument auf der Dateihostingplattform. BITTE UMGEHEND LÖSEN." Sie atmen tief ein und aus, nehmen einen Schluck Kaffee (oder am besten gleich zwei) und bereiten sich darauf vor, im Laufe der nächsten 30 Minuten die Konfiguration zu überprüfen und fünf verschiedene Bildschirme aufzurufen, um eine einfache URL-Ausnahme festzulegen. Aufgrund der immer weiter steigenden Zahl von Einstellungen, Befehlen und ungleichartigen Tools kommt es recht häufig vor, dass Netzwerkadministratoren ihre wertvolle Zeit für solche Aufgaben opfern müssen.

Gehen wir einfach einmal davon aus, dass Sie drei verschiedene E-Mail-Konten haben (also je eine geschäftliche und private E-Mail-Adresse und ein weiteres Konto für Werbung). So ist es relativ einfach, den Überblick zu behalten und wirklich wichtige E-Mails („Omas 80. Geburtstag", eine Mitteilung vom Chef usw.) von Spam zu unterscheiden. Doch was glauben Sie, wie einfach das bei 100 Konten wäre, die alle hin und wieder E-Mails mit wichtigen Informationen enthalten? Wahrscheinlich wäre das nicht so einfach.

Schon gewusst?

Mit RapidDeploy haben die Kunden von WatchGuard seit 2012 mehr als **16 Jahre Arbeit** eingespart.

Einfach

Zentrale Verwaltung:

Investieren Sie in leicht konfigurierbare, schnell implementierbare und einfach zu verwaltende Produkte

Die Lösung: Ihre Arbeitslast ist auch ohne die ständigen Sicherheitswarnungen und die zahlreichen Bildschirme, die Sie überwachen müssen, groß. Entscheiden Sie sich daher für Netzwerksicherheitsprodukte, die die fortlaufende Verwaltung über eine intuitive Oberfläche ermöglichen. WatchGuard Firebox Appliances sind nicht nur einfach zu konfigurieren und bereitzustellen: Bei ihrer Entwicklung lag besonderes Augenmerk auf einer zentralen Steuerung über eine Konsole, um so auch im laufenden Betrieb die Regel- und Netzwerkverwaltung zu vereinfachen.

Leichte Konfiguration: Durch die One-Touch-Konfiguration oder -Aktualisierung der Firmware von allen WatchGuard Appliances sparen Sie Zeit und sorgen dafür, dass die Richtlinien über die gesamte Organisation hinweg synchronisiert werden. Sie können von jedem Ort aus flexibel Policy-Vorlagen erstellen und anhand rollenbasierter Mandanten schnell auf mehrere Appliances übertragen.

Reibungslose Bereitstellung: WatchGuard RapidDeploy ist ein leistungsstarkes, Cloud-basiertes Bereitstellungs- und Konfigurationswerkzeug und gehört zum Lieferumfang aller WatchGuard Firebox Appliances. Sie müssen die Appliance lediglich einschalten und mit dem Internet verbinden. Den Rest können Sie von jedem beliebigen Standort aus erledigen.

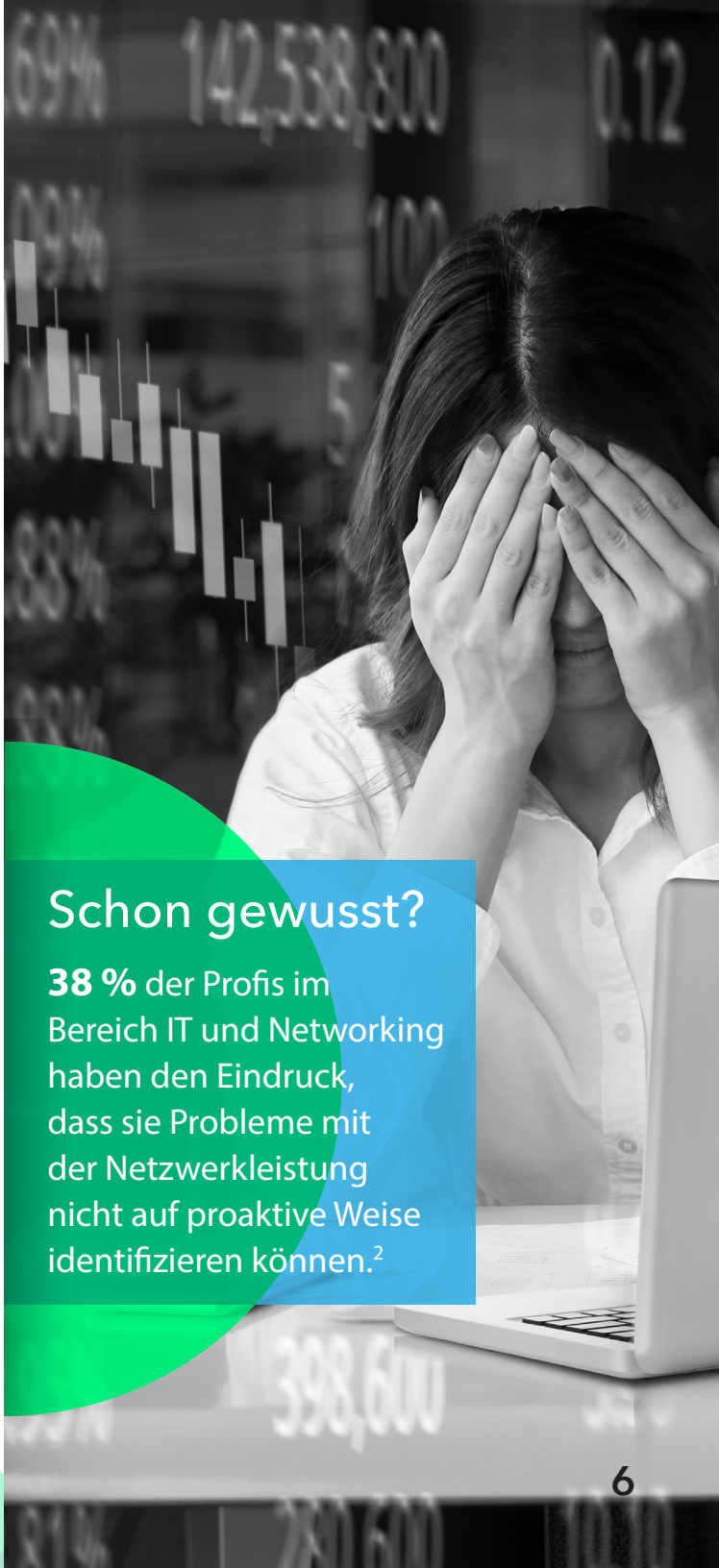
Einfaches Management: Egal ob eine oder Hunderte Firebox-Appliances: Die Verwaltung erfolgt über eine benutzerfreundliche Konsole – für maximale Effizienz und eine schlanke Netzwerkadministration. Dank einer übersichtlichen, visuell ansprechenden Oberfläche und leicht verständlichen Protokollnachrichten ist es völlig unkompliziert, die Sicherheit und Compliance jederzeit zu gewährleisten.

Kompliziert

Manuelle Datenanalyse

Heutzutage sind IT-Infrastrukturen immer größer und komplexer. Daher ist es äußerst wichtig, detaillierte Informationen zu den Netzwerkaktivitäten zu erhalten, die die IT-Teams nutzen können, um Muster, Bedrohungen und Sicherheitslücken zu erkennen und rechtzeitig zu handeln. Diese Daten sind zwar sehr wertvoll, doch sie müssen auch zeitnah abrufbereit und handlungsrelevant sein, damit sie für das Sicherheitsteam von Nutzen sind.

Viele aktuell erhältliche Visualisierungslösungen stellen große Mengen an Daten bereit. Der Haken ist, dass sie nicht der Wichtigkeit nach sortiert werden. Für die meisten Teams ist der dadurch entstehende Arbeitsaufwand einfach zu hoch, denn sie müssen auch so unzähligen Sicherheitswarnungen nachgehen. Es liegt jedoch außerhalb des Möglichen, alle zu untersuchen oder zu priorisieren. Wirklich leistungsstarke Visualisierungsprodukte zeichnen sich dadurch aus, dass sie die vorherrschenden Bandbreiteneinschränkungen erkennen und die wichtigsten Vorfälle hervorheben, um so die Netzwerksicherheit zu garantieren.



Schon gewusst?

38 % der Profis im Bereich IT und Networking haben den Eindruck, dass sie Probleme mit der Netzwerkleistung nicht auf proaktive Weise identifizieren können.[2]

Einfach

Handlungsrelevante Daten:

Verwenden Sie automatisierte Visualisierungs- und Reporting-Lösungen

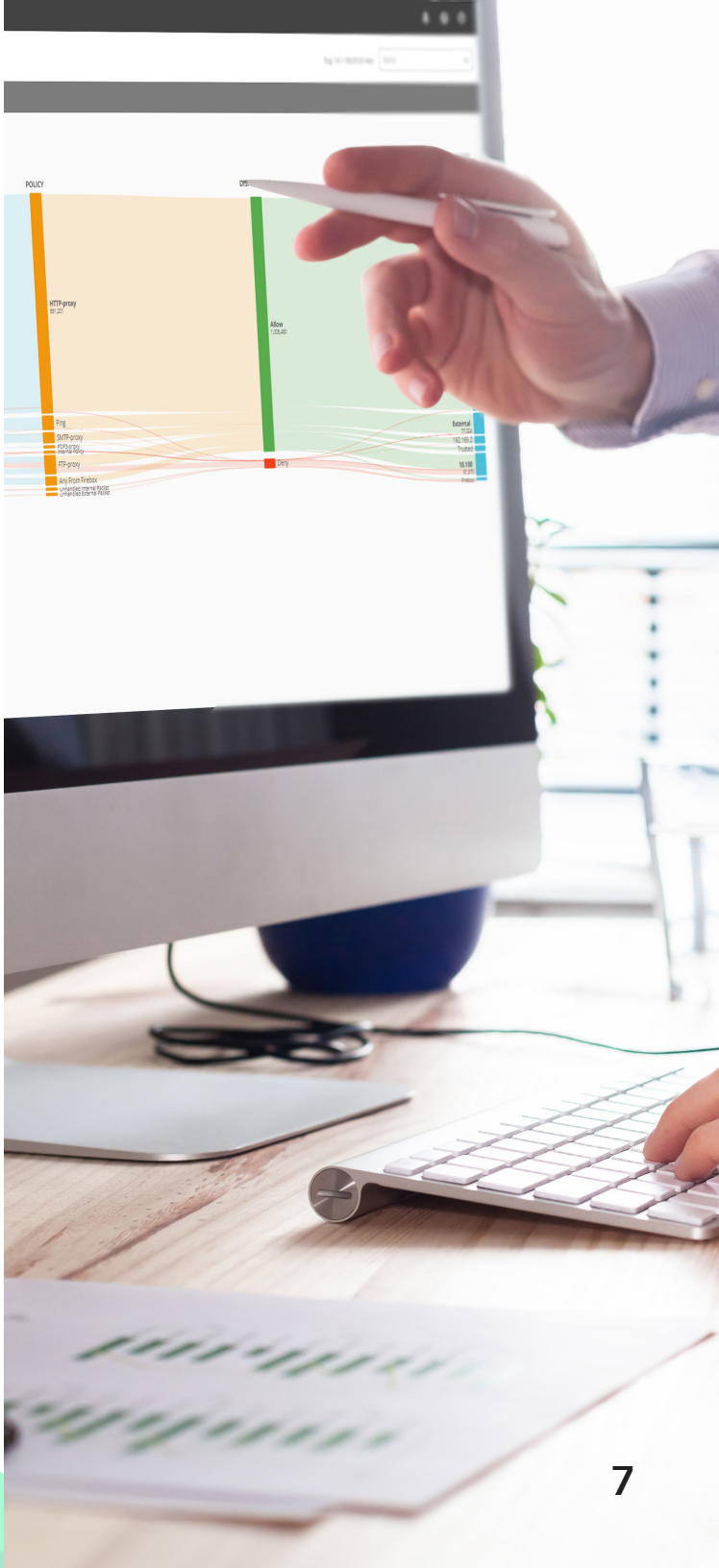
Die Lösung? Ein automatisiertes, intuitives Berichtsdashboard trägt dazu bei, dass Ihr IT-Team nicht allzu viel Zeit für risikoarme Vorfälle opfert. WatchGuard Cloud Visibility bietet zeitnahe, zuverlässige und relevante Daten, sodass IT-Teams umgehend Muster erkennen und informierte Entscheidungen treffen können. Dank den integrierten Dashboards und Berichtsfunktionen erhalten Sie schnell Informationen zu Sicherheitsvorfällen, Compliance-Audits und Mustern im Netzwerk. Mit einer Cloud-Plattform können Sie überall und jederzeit in Echtzeit die Netzwerksicherheit überwachen und wichtige Einblicke erhalten. Hinzu kommt, dass keine Hardware-Infrastruktur erforderlich ist. Einfacher geht's nicht, oder?

WatchGuard Cloud Visibility stellt Informationen zum Netzwerk für die Führungsebene zur Verfügung, wie:

- Hauptbenutzer
- Hauptziele
- Hauptanwendungen
- Haupt-Domains

Sie können auch aktuelle Sicherheitsinformationen aufrufen, darunter:

- Blockierte Haupt-Botnet-Sites
- Blockierte Hauptclients und -ziele
- Blockierte erweiterte Haupt-Malware-Angriffe
- Intrusion Prevention



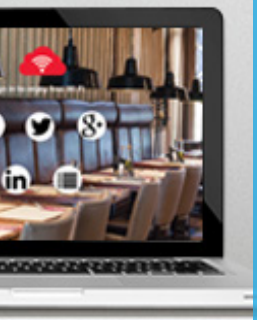
Kompliziert

Unsicheres, leistungsschwaches WLAN

WLAN bietet modernen Unternehmen viele Vorteile – beispielsweise ist es maßgeblich für Programme wie Bring Your Own Device (BYOD) und Mitarbeitermobilität – doch es öffnet auch Bedrohungen die Tür zu Ihrem Unternehmensnetzwerk. Denn heutzutage findet man im Internet Informationen unterschiedlichster Art dazu, wie ein WLAN-Netzwerk gehackt wird, einschließlich detaillierter Anleitungsvideos auf YouTube. Dies führt dazu, dass selbst unerfahrene Cyberkriminelle ihr Glück versuchen und sich die sechs bekannten Hauptbedrohungen ausweiten.

Evil Twin Access Point | **Rogue-Client** | **Fehlerhaft konfi-gurierter Access Point** | **Benachbarter Access Point** | **Rogue Access Point** | **Ad-hoc-Netzwerk**

Viele Ressourcen in IT-Abteilungen sind bereits damit beschäftigt, WLAN-bezogene Probleme wie vergessene Passwörter für mobile Apps, E-Mail-Synchronisierungsfehler und Störungen beim Zugriff auf WLAN-Netzwerke zu beheben. Die Folge ist, dass die meisten Unternehmen einfach nicht über ausreichend Bandbreite verfügen, um Lösungen für alle sechs WLAN-Bedrohungen zu implementieren – geschweige denn diese zu verwalten. Sie benötigen eine umfassende Lösung, die nicht nur einfach bereitgestellt und verwaltet werden kann, sondern auch die Leistungsanforderungen ihrer Umgebung erfüllt und gleichzeitig vor allen WLAN-Bedrohungen schützt.



Schon gewusst?

Ein durchschnittlicher Mitarbeiter, der an einem BYOD-Programm (Bring Your Own Device) teilnimmt, spart dank des eigenen Mobilgeräts pro Woche 37 Minuten Arbeitszeit ein.[3]

Einfach

Stabileres, sichereres WLAN:

Setzen Sie auf Trusted Wireless Environment, ein vertrauenswürdiges WLAN-Konzept

Die Lösung: Eine effiziente, sichere WLAN-Konnektivitätslösung muss nicht unbedingt komplex sein. WatchGuard ist das einzige Unternehmen, das ein von Miercom verifiziertes Framework für den Aufbau eines leistungsstarken, unkomplizierten WLAN-Netzwerks bietet, das gegen alle sechs bekannten Hauptbedrohungen gesichert ist. Nutzer von WatchGuard Secure Cloud profitieren außerdem von WatchGuard Discover, einer in die Wi-Fi Cloud integrierten App, die die Leistung und den Zustand des Netzwerks überwacht und wertvolle Einblicke ermöglicht. Im Lieferumfang von Discover sind eine Reihe handlungsrelevanter Funktionen für die Visualisierung, Problembehebung und die Überprüfung des Netzwerkzustands enthalten, darunter:

Client Journey: ein Live-Snapshot für alle Ihre Standorte, sodass Sie immer darüber informiert sind, ob Kunden Probleme bei der Zuordnung, Authentifizierung oder generell mit dem Netzwerk haben, die nicht auf das WLAN zurückgehen.

Network Baselining: die Performance, Konnektivität und Anwendungserfahrung aller Kunden und AP in der Reichweite Ihrer Netzwerke wird überwacht, um normale und anormale Ereignisse zu identifizieren. Wird eine Anomalie aufgespürt, können Sie mit Discover die Grundursache ermitteln. Außerdem empfiehlt Ihnen diese Funktion konkrete Maßnahmen, um die Netzwerkprobleme zu beheben – selbst solche, die nicht mit dem WLAN zusammenhängen.

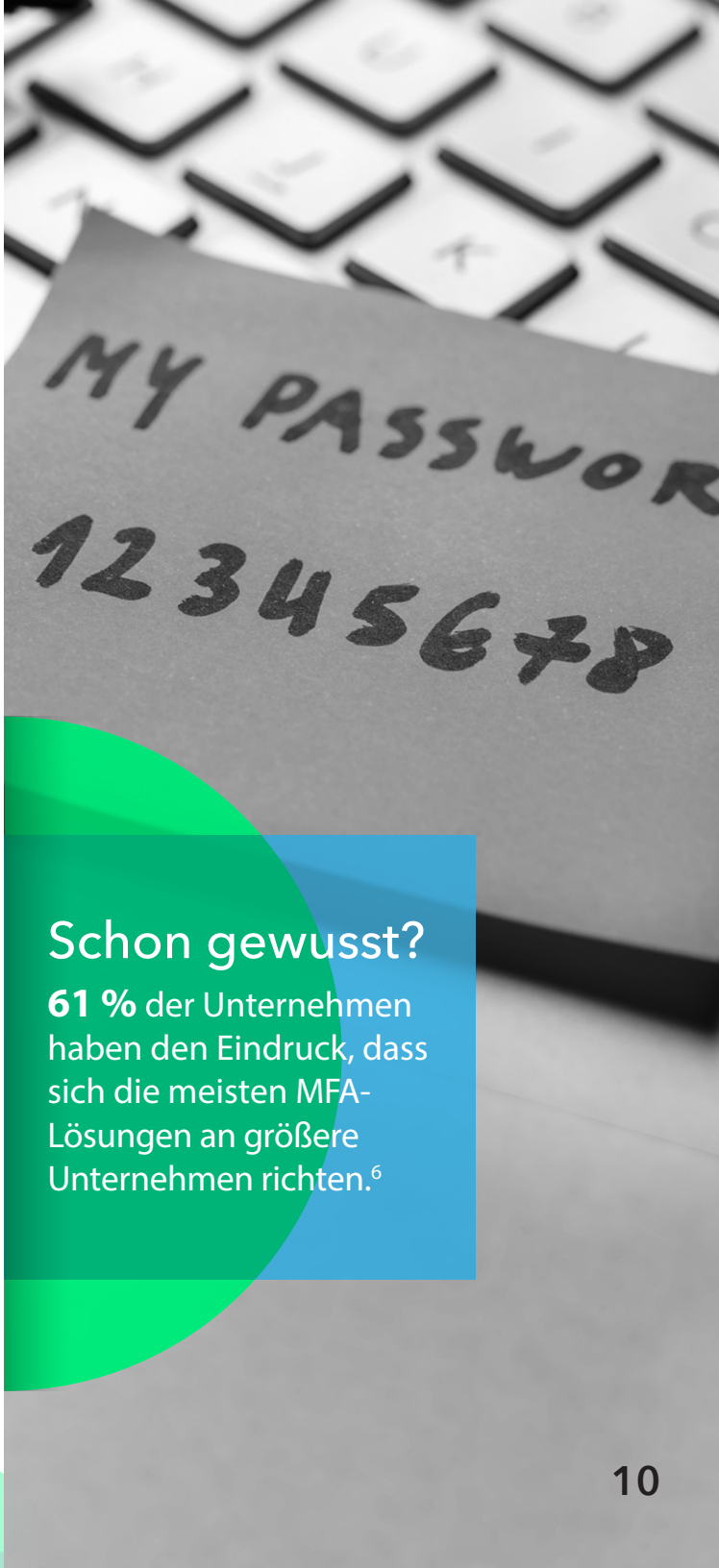
Warnmeldungen: Mit der Warnmeldefunktion von Discover ist die Erfüllung von Service Level Agreements (SLAs) ein Kinderspiel. Sie können dazu beitragen, dass das WLAN sowie alle Ihre drahtgebundenen und Anwendungsnetzwerkressourcen reibungslos funktionieren.

Kompliziert

Aufwendige Einführung von MFA-Lösungen

Eine der größten Herausforderungen für Unternehmen ist heutzutage die Passwortsicherheit. Unfassbare **81 % der Datensicherheitsverletzungen rühren von schwachen oder gestohlenen Passwörtern her**[4]. Da ist es nicht verwunderlich, dass Unternehmen die Vor- und Nachteile von Produktlösungen für die Multifaktor-Authentifizierung gegenüberstellen – mit dem Ziel, den Schutz unternehmensinterner Ressourcen zu verstärken.

Einige dieser Produkte, die von IT-Teams getestet wurden, stellten sich als sehr komplex heraus. Bei der Einführung von herkömmlichen Hardware-basierten MFA-Lösungen ist der Zeit- und Ressourcenaufwand hoch. Letztendlich hat dies zur Folge, dass die Implementierung mit anderen Prioritäten nicht vereinbar ist – und erst recht nicht mit den eingehenden Support-Tickets. Hinzu kommt, dass das IT-Team und die Mitarbeiter in den meisten Fällen auch speziell geschult werden müssen, schließlich ist die mangelnde Nutzerfreundlichkeit eine der größten Beschwerdeursachen bei traditionellen Lösungen. **24 % der Unternehmen, die keine MFA-Lösung verwenden, gaben tatsächlich an, dass die komplizierten Implementierungs-, Wartungs- und Unterstützungsprozesse sie von der Einführung abhalten**[5]**.**



Schon gewusst?

61 % der Unternehmen haben den Eindruck, dass sich die meisten MFA-Lösungen an größere Unternehmen richten.[6]

Einfach

Cloud-basierte MFA:

Identitätsprüfung ganz ohne Hardware und Komplikationen

Die Lösung? Ein MFA-Service, der nicht nur ganz leicht und kostengünstig bereitgestellt wird, sondern auch intuitiv und benutzerfreundlich ist, sodass alle Mitarbeiter unabhängig vom technischen Know-how damit zurechtkommen. WatchGuard AuthPoint bietet Multifaktor-Authentifizierung (MFA) auf einer benutzerfreundlichen Cloud-basierten Plattform. Da sich die Lösung in der Cloud befindet, müssen Sie keine Hardware bereitstellen, und der Zugriff kann von jedem beliebigen Ort aus verwaltet werden. Die mobile App zeigt jeden Anmeldeversuch an und erleichtert es den Benutzern, Anmeldungen zu genehmigen oder zu verweigern. AuthPoint kann außerdem in zahlreiche Drittanbieteranwendungen integriert werden, etwa gängige Cloud-Anwendungen, Webdienste, VPNs und Netzwerke.

Einfach

Delegierung:

Schließen Sie sich mit einem MSSP (Managed Security Service Provider) zusammen

Alle WatchGuard Produkte wurden so konzipiert, dass sie möglichst einfach zu verwenden sind, damit Sie sich auf die wirklich wichtigen Dinge konzentrieren können. Wenn Sie jedoch überhaupt keine Kapazitäten für die unternehmensinterne Verwaltung der Sicherheit haben, können Sie sich voll und ganz auf einen unserer Anbieter von IT-Lösungen verlassen. Die WatchGuard Lösungsanbieter sind eine Erweiterung der eigenen Organisation und füllen so mögliche Lücken in der IT, indem sie Verwaltungsdienstleistungen wie die Bereitstellung, fortlaufende Wartung, Berichterstellung usw. anbieten.

Dank des Partner Finder-Tools (watchguard.com/findapartner) von WatchGuard ist es jetzt so einfach wie nie, einen MSSP in Ihrer Nähe zu finden. Mit den Filteroptionen können Sie nach Standort oder Spezialisierung suchen, um so den am besten geeigneten Partner mit WatchGuard-Zertifizierung zu finden.

Fazit

Zeitliche und personelle Einschränkungen erschweren erheblich die Verwaltung der IT-Sicherheit im Unternehmen. An dieser Stelle kommt WatchGuard ins Spiel. Unsere Lösungen wurden speziell so konzipiert, dass sie kinderleicht zu konfigurieren, bereitzustellen und zu managen sind. Das Netzwerkmanagement ist komplex genug, die Sicherheit muss es nicht auch noch sein.

Netzwerksicherheit

Unsere Plattform stellt nicht nur Sicherheit auf Enterprise-Niveau bereit, sondern ist von Grund auf so konzipiert, dass der Fokus auf einer einfachen Bereitstellung, Verwendung und fortlaufenden Verwaltung liegt. Dies macht WatchGuard zur idealen Lösung für KMUs, mittelständische Unternehmen und dezentrale Großkonzerne weltweit.

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

WatchGuard AuthPoint® ist die ideale Lösung, um die Lücke bei der passwortgestützten Sicherheit zu schließen und so Unternehmen wirkungsvoll vor Sicherheitsverletzungen zu schützen. Die Lösung bietet Multi-Faktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform. Bei der einzigartigen Lösung 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.

Einen Partner suchen >

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 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 kleine und mittlere sowie 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 Pazifikraum. Weitere Informationen finden Sie unter WatchGuard.de.

[1] StationX, „Predictions for 2019: Cybersecurity skills shortages are getting worse", Januar 2019
[2] APM Digest, „Here's why IT teams spend too much time on network troubleshooting", März 2019
[3] Information Age, „The relationship between Wi-Fi and BYOD culture", April 2017
[4] CSO, „Hacked passwords cause 81% of data breaches", Mai 2017
[5] WatchGuard, „Passwords have failed, so what's next?", Mai 2018
[6] WatchGuard, „Passwords have failed, so what's next?", Mai 2018

WatchGuard

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