AuthPoint

MFA - Große Stärken leicht gemacht

Die Verwendung gestohlener Anmeldedaten, um unerlaubt auf Netzwerkressourcen zuzugreifen, ist die beliebteste Taktik von Hackern.* Da neben einem einfachen Passwort ein zusätzlicher Identitätsnachweis erforderlich ist, ist die Multifaktor-Authentifizierung die wichtigste Sicherheitsmaßnahme für Ihr Unternehmen.

Die einzigartige Lösung für die Multifaktor-Authentifizierung (MFA) von WatchGuard reduziert zum einen mit schwachen oder gestohlenen Anmeldedaten einhergehende Netzwerkausfälle und Sicherheitslücken. Gleichzeitig erfolgt die Bereitstellung vollständig über die Cloud, was die Einrichtung und Verwaltung vereinfacht. AuthPoint geht zudem über die herkömmliche Zwei-Faktor-Authentifizierung (2FA) hinaus, indem innovative Methoden der Benutzeridentifizierung eingesetzt werden – wie beispielsweise bei unserem Ansatz, die DNA des Mobilgeräts zu überprüfen. Mit unserem umfangreichen Eco-System, bestehend aus Integrationen von Drittanbietern bedeutet dies einen starken Schutz für das Netzwerk, VPNs, Cloud-Anwendungen usw. – wo auch immer Bedarf besteht. Selbst für Laien ist die benutzerfreundliche mobile AuthPoint-App einfach zu verwenden und praktisch. WatchGuard AuthPoint ist letztendlich die richtige Lösung zum richtigen Zeitpunkt, um MFA für Unternehmen zu ermöglichen, die sie dringend benötigen, um Angriffe abzuwehren.

Effizienter MFA-Schutz über DNA des Mobilgeräts

Bei der Multi-Faktor-Authentifizierung müssen Benutzer ihnen bekannte Informationen (Benutzername und Passwort), Geräte und andere (mit ihnen verknüpfte) Faktoren nutzen. AuthPoint bietet ein äußerst sicheres MFA-Produkt und verwendet Push-Nachrichten, QR-Codes oder Einmalkennwörter (One-Time Passwords, OTPs). Und die Mobilgeräte DNA Smartphones gleicht sich beim Zugriff auf Systeme und Anwendungen mit dem Telefon des autorisierten Benutzers ab. Daher würde jeder Angreifer, der ein Benutzergerät klont und versucht, auf ein geschütztes System zuzugreifen blockiert, da sich die Geräte-DNA unterscheidet.

Benutzerfreundliche mobile AuthPoint-App

Die AuthPoint-App von WatchGuard ermöglicht es Benutzern, sich direkt über ihr Telefon zu authentifizieren! Sie benötigen keine Key Fobs oder USB-Sticks; Sie können die AuthPoint-App in Sekunden installieren und aktivieren und sie dann für die Authentifizierung über ein Smartphone verwenden. Die App ermöglicht eine schnelle Push-basierte Authentifizierung sowie Offline-Authentifizierung mit QR-Codes über die Telefonkamera. Sie ist in 11 Sprachen verfügbar und kann kostenlos im App Store und bei Google Play heruntergeladen werden.

Umfassende Abdeckung mit Web-SSO

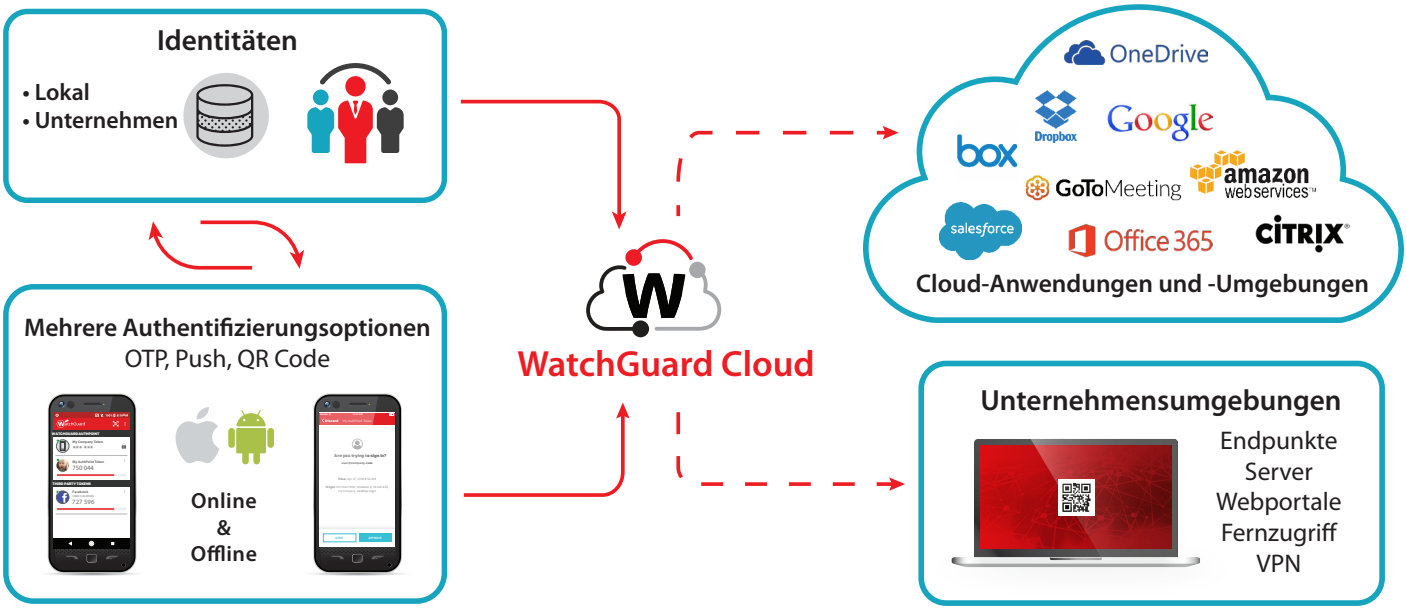
Das EcoSystem von WatchGuard umfasst Dutzende von Drittanbieterintegrationen mit AuthPoint. Unternehmen können Benutzer also auffordern, sich zu authentifizieren, bevor sie auf sensible Cloud-Anwendungen, VPNs und Netzwerke zugreifen. AuthPoint unterstützt den SAML-Standard. Mit einer Anmeldung können Benutzer auf eine breite Palette an Anwendungen und Diensten zugreifen. Daneben ermöglicht die sichere Anmeldefunktion Online- und Offline-Authentifizierung bei Windows- und Mac-Rechnern unter Verwendung der AuthPoint-App.

Cloud-basierter Dienst zu geringen Gesamtbetriebskosten (TCO)

Unternehmen mit wenigen IT-Mitarbeitern und geringem Sicherheits-Know-how profitieren von MFA-Schutz, der einfach über die Cloud bereitgestellt und verwaltet werden kann. AuthPoint wird auf der WatchGuard Cloud-Plattform ausgeführt und ist überall verfügbar. Sie müssen keine Software installieren, Upgrades planen oder Patches verwalten. Ferner stellt die Plattform problemlos eine Ansicht eines einzelnen globalen Accounts oder vieler unabhängiger Accounts bereit, sodass dezentrale Unternehmen und Managed Service Provider nur die Daten anzeigen können, die für die Rolle einer Person relevant sind.

**Verizon Data Breach Investigations Report 2018*

Schützen Sie Netzwerk, VPNs, Cloud-Ressourcen und mehr vor Betrügern!



WatchGuard Cloud-Plattform

- 100 % Cloud-basierte Verwaltung
- Authentifikatorzuweisung und -aktivierung
- Authentifizierungsrichtlinien basierend auf Gruppen und Ressourcen
- Protokolle und Berichte
- Rollenbasierte Zugriffssteuerung
- Intuitive, attraktive Benutzeroberfläche

Mobile AuthPoint-App

- Drei Authentifizierungsmethoden in einer:
  1. Push-Nachrichten
  2. Einmalkennwörter
  3. QR-Codes (offline)
- Mobiler Authentifikator – keine zusätzliche Hardware erforderlich
- 11 Sprachen
- Unterstützung mehrerer Token
- iOS und Android – kostenloser Download
- Schutz durch PIN/biometrische Daten (auf bestimmten Geräten)
- DNA des Mobilgeräts – zusätzlicher Authentifizierungsfaktor
- Mobile Token-Migration (Self-Service) zu neuen Geräten

AuthPoint-Gateway

- Netzwerk-Gateway für Unternehmen
- Benutzerauthentifizierung und -synchronisierung (AD und LDAP)
- RADIUS-Proxy

AuthPoint-Agenten

- Integration mit Drittanbieteranwendungen ohne native MFA-Unterstützung
- Anmeldeschutz für Windows und macOS

AuthPoint-Ökosystem

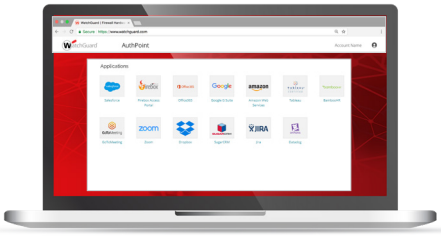
- MFA für Ressourcen, Anwendungen, Datenbanken und Webressourcen in der Cloud
- Unterstützung für SAML- und RADIUS-Standards
- Umfassende Integrationsleitfäden für viele gängige Drittanbieterlösungen

Empfohlene Anwendungsfälle

VPNs/Fernzugriff

Selbe Benutzererfahrung wie Benutzername + Passwort, ABER sicherer und mit Bestätigung per Klick.

1. Verbindung mit Benutzername & Passwort anfordern
2. VPN-Verbindung bestätigen – Anfrage über AuthPoint-App



Cloud-Anwendungen – Web-SSO

1. Auf das Identitätsportal (IdP) zugreifen
2. Mit OTP, Push oder QR-Code authentifizieren
3. Auf alle Apps zugreifen, für die Sie eine Berechtigung haben – keine erneute Authentifizierung erforderlich!

PC-Anmeldung – Online-Authentifizierung

1. Auf „Push senden“ klicken
2. PC-Anmeldung bestätigen – Anfrage über AuthPoint-App
3. Anmeldung erfolgreich

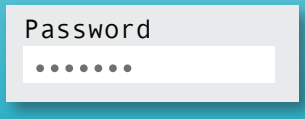
PC-Anmeldung – Offline-Authentifizierung

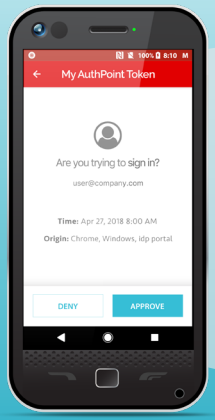
1. „QR-Code“ für Authentifizierung auswählen
2. QR-Code mit AuthPoint -App scannen
3. Antwort 717960 eingeben (in diesem Beispiel)

Was ist Multi-Faktor-Authentifizierung (MFA)?

Verwendung von 2 oder mehr Authentifizierungs- faktoren:

- **Informationen** (Passwort, PIN)
- **Gerät** (Token, Smartphone)
- **Körperteil** (Fingerabdruck, Gesicht)





AuthPoint-Faktoren:

1. **Ihr Passwort**
2. **Genehmigung auf Ihrem mobilen Authentifikator**
3. **Korrekte DNA des Smartphones**
4. **Fingerabdruck für Zugriff** (bei bestimmten Telefonmodellen)

AuthPoint hält das Versprechen der MFA. Die App reduziert das Geschäftsrisiko im Zusammenhang mit 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

Argumente für MFA

Wenn die direkten und Berücksichtigt man die direkten und indirekten Ausgaben, die mit einer Sicherheitslücke in Verbindung stehen, so können sich die Kosten summieren. Sobald eine Sicherheitslücke aufgedeckt wurde, werden oftmals Spezialisten hinzugezogen, , um die Ursache der zu ermitteln, Sicherheitsmaßnahmen zu ergreifen, um Schwachstellen zu beseitigen, Bußgelder oder Rechtstreitkosten zu bezahlen. Die indirekten Kosten durch eine geringere Mitarbeiterproduktivität und verlorene bestehende und zukünftige Kunden können allerdings noch substantieller sein. Um eine Zahl zu nennen: Eine Studie des Ponemon Institute[1] beziffert die **durchschnittlichen Kosten einer Sicherheitslücke auf 141 USD pro Datensatz** für sensible Daten…oder 1,32 Millionen USD bei einer durchschnittlichen Sicherheitsverletzung mit 9.350 Datensätzen.

Wie wahrscheinlich ist es, dass eine Sicherheitsverletzung durch ein schwaches oder geteiltes Passwort auftritt? Daten zeigen, dass 3 von 100 Personen[2] das schwache Passwort „123456" und **6 von 100 Personen dasselbe Passwort für alle Online-Zugänge verwenden**. Sie müssen sich also fragen, wie wahrscheinlich es ist, dass ein oder mehrere ihrer Mitarbeiter nicht sorgfältig mit Passwörtern umgehen.. Dies mag ein Grund sein, warum immer mehr Kontrollorgane eine 2FA oder MFA, zumindest für den Teil der Benutzer fordern, die Compliance-Richtlinien oder Payment Card Industry Data Security Standard (PCI-DSS v 3.2) unterliegen.

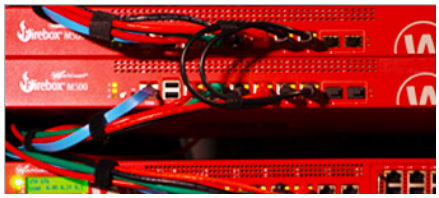
Die gute Nachricht ist, dass Sie diese Risiken mit Cloud-basierter Multifaktor-Authentifizierung im angemessenen Rahmen minimieren können. Es fallen keine Ausgaben für zusätzliche Infrastruktur, Hardware-Token sowie Softwaresupport und -wartung an. Zudem kostet es nur **2,50 USD pro Benutzer pro Monat** oder weniger, das Risiko in Höhe von 1,32 Millionen USD zu reduzieren.

1 2017 Ponemon Institute Cost of Data Breach Study und 2017 Ponemon State of SMB Cybersecurity Report

2 http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

3 https://www.statista.com/statistics/763091/us-use-of-same-online-passwords

WATCHGUARD-SICHERHEITSPORTFOLIO



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

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 wird sichergestellt, dass nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen erhält.

Mehr erfahren

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **https://www.watchguard.com**.

Über WatchGuard

WatchGuard® Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen von WatchGuard profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält WatchGuard Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter **WatchGuard.de**.