AuthPoint

MFA - Große Stärken leicht gemacht

Die heutige Sicherheitslandschaft zeigt, dass die Verwendung gestohlener Anmeldedaten, um unerlaubt auf Netzwerkressourcen zuzugreifen, die beliebteste Taktik von Hackern ist. Tatsächlich stellen bei 80 % der Datensicherheitsverletzungen gestohlene oder schwache Kennwörter die größte Schwachstelle dar.* Die Multifaktor-Authentifizierung ist die wichtigste Sicherheitsverbesserung zum Schutz Ihres Unternehmens.

Die Lösung für die Multifaktor-Authentifizierung (MFA) von WatchGuard schützt Identitäten, reduziert mit schwachen oder gestohlenen Anmeldedaten einhergehende Netzwerkausfälle und Sicherheitslücken und bietet diese Funktionen vollständig über die Cloud, was die Einrichtung und Verwaltung stark vereinfacht. Die einzigartige, mobile DNA-Technologie von AuthPoint geht zudem über die herkömmliche Zwei-Faktor-Authentifizierung (2FA) hinaus, indem innovative Methoden für Identifizierung und Schutz eingesetzt werden. Unser umfangreiches Ökosystem aus Integrationen mit mehr als 130 Drittanbietern bedeutet einen durchgängig starken Schutz für das gesamte Netzwerk, VPNs und Cloud-Anwendungen – 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.

Risikoauthentifizierung für Zero-Trust-Implementierung

Für die Zero-Trust-Implementierung ist ein Identitätsschutz erforderlich, und da die risikobasierte Authentifizierung ein Kernelement von MFA ist, ist AuthPoint die Schlüssellösung für den Ansatz „never trust, always verify" (niemals vertrauen, immer prüfen). Ohne bestehende Risikorichtlinien müsste Ihr Unternehmen jederzeit und für alle Anwender die sicherste Authentifizierungsmethode aktivieren, was in einigen Segmenten zu unnötig hohem Aufwand für die Anwender führen könnte. Mit AuthPoint haben Sie ohne zusätzliche Kosten Zugriff auf Risikofunktionen, darunter Netzwerkstandorte, Zeitpläne, Geolokalisierung und die exklusive mobile DNA, um das Cloning mobiler Token zu verhindern.

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.

Große Reichweite mit SSO im Web

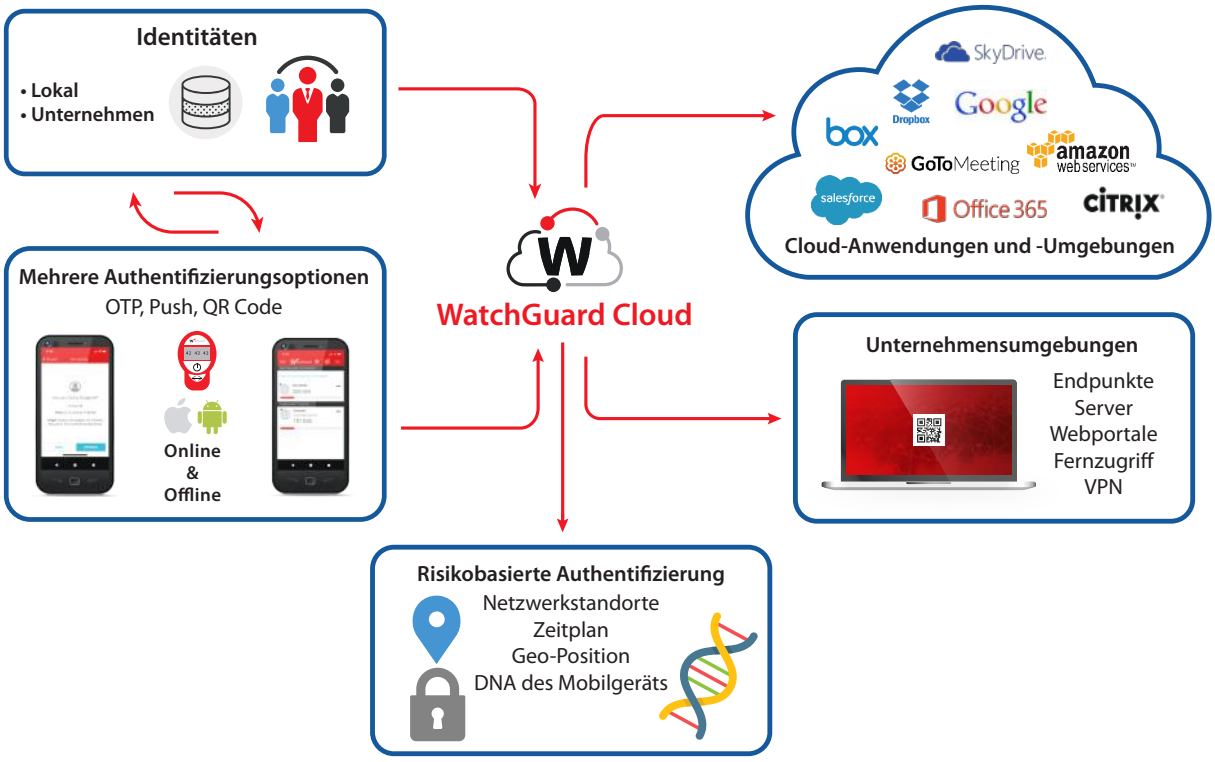
Sie müssen sich nicht zahllose komplexe Kennwörter mehr merken. Die sichere Single-Sign-On-Funktion (SSO) von AuthPoint sorgt dafür, dass Anwender einfacher auf mehrere Cloud-Anwendungen, VPNs und Netzwerke zugreifen können – mit denselben Anmeldedaten. Dadurch lassen sich die Herausforderungen meistern, die die Kennwort-Ermüdung mit sich bringt. Zudem wird das Risiko von Sicherheitsschwachstellen aufgrund schwacher Kennwörter gesenkt und Kosten werden verringert, die mit dem Zurücksetzen von Kennwörtern einhergehen. AuthPoint unterstützt das SAML-Standardprotokoll. 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 oder Hardware-Token.

Anwenderfreundliche, optimierte, mobile App

Installieren und aktivieren Sie die AuthPoint-App von WatchGuard in Sekundenschnelle, um die Authentifizierung von Ihrem Smartphone aus vorzunehmen. Sie bietet nicht nur eine schnelle, Push-basierte Authentifizierung, sondern auch eine Funktion für die Pull-Authentifizierung für bessere Bedienbarkeit und Sicherheit. Die App ermöglicht auch eine Offline-Authentifizierung mithilfe von QR-Codes über die Telefonkamera. Sie ist in 13 Sprachen verfügbar und kann kostenlos im App Store und bei Google Play heruntergeladen werden.

**Verizon Data Breach Investigations Report 2020*

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



WatchGuard Cloud-Plattform

- 100 % cloudbasierte Verwaltung in drei Regionen
- Leistungsstarke, risikobasierte Richtlinienverwaltung
- Protokolle und Berichte
- Audit des rollenbasierten Zugriffs
- Intuitive, attraktive Benutzeroberfläche

Mobile AuthPoint-App

- Drei Authentifizierungsmethoden in einer:
  1. Push-Nachrichten mit garantierter Zustellung
  2. Einmalkennwörter
  3. Challenge/Response-QR-Codes
- Mobiler Authentifikator – keine zusätzliche Hardware erforderlich
- 13 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
- Unterstützung der Token von Drittanbietern, um persönliche Konten zu schützen (Gmail, soziale Medien usw.)

AuthPoint-Gateway

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

AuthPoint-Agenten

- Integration mit Drittanbieteranwendungen ohne native MFA-Unterstützung
- Online-, Offline- und RDP-Anmeldeschutz für Windows und macOS
- Agent für RD Web und ADFS

AuthPoint-Ökosystem

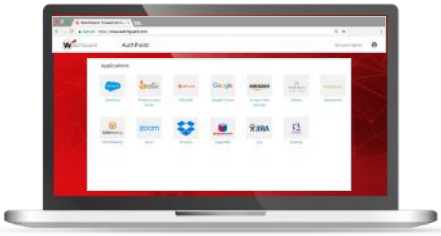
- Integration mit Drittanbieteranwendungen ohne native MFA-Unterstützung
- Unterstützung für SAML- und RADIUS-Standards
- Anleitungen für Integrationen mit mehr als 130 Drittanbietern, darunter CRM- und Videokonferenzlösungen
- Direkte Integration von Firebox mit AuthPoint für eine schnelle VPN-Konfiguration
- AuthPoint Hardware-Token ohne Offenlegung von Token-Seed sowie Support für Hardware-Token von Drittanbietern (OATH TOTP)

Empfohlene Anwendungsfälle

VPNs/Fernzugriff

Selbe Benutzererfahrung wie Benutzername + Passwort, ABER sicherer und mit Bestätigung per Klick. Integration mit sämtlichen Firewalls, aber insbesondere mit einsatzbereiten Firebox-Anwendungen.

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. Greifen Sie auf alle Ihnen zugewiesenen Apps zu – mit nur einem Kennwort. Es ist keine erneute Authentifizierung erforderlich!

PC-Anmeldung oder RDP-Verbindung

1. Melden Sie sich mit Ihren Anmeldedaten bei Windows/Mac an
2. Wählen Sie die bevorzugte Authentifizierungsmethode aus (Push, QR-Code oder OTP)
3. Genehmigen Sie die Methode auf Ihrem Smartphone. Anmeldung abgeschlossen!

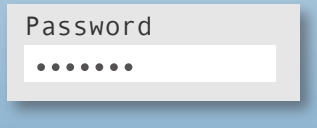
PC-Anmeldung – Offline-Authentifizierung

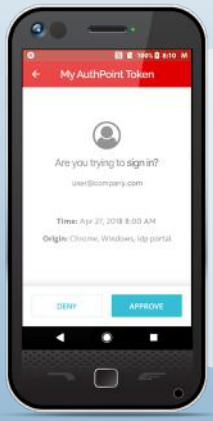
1. Melden Sie sich mit Ihren Anmeldedaten bei Windows/Mac an
2. Scannen Sie den QR-Code (oder OTP) mit der AuthPoint-App
3. Antwort 717960 eingeben (in diesem Beispiel)

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 bestimmtenTelefonmodellen)

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

Reduzieren Sie Ihre Risiken mit MFA

Schwache Passwörter sind ein großes Risiko für Ihr Unternehmen. **Der durchschnittliche Benutzer hat fast 100 Onlinekonten**, viele davon mit eigenen Passwortanforderungen. Passwort-Ermüdung ist ein reales Problem und gefährdet Ihr Unternehmen. Ein schwaches oder geknacktes Passwort reicht aus, damit ein Cyberkrimineller auf all Ihre Daten und Konten zugreifen kann.

Wie sicher sind Sie, dass jeder einzelne Mitarbeiter die Best Practices für Passwörter befolgt?

- Rund 250.000 Passwörter werden täglich gestohlen[1]
- Nur 1 von 5 Benutzern verwendet für alle Konten ein anderes Passwort[2]
- 3 % der Mitarbeiter verwenden das Passwort 1234563[3]

> 2021 werden Unternehmen, die den Remote-Zugriff schnell ausweiten, ohne MFA zu implementieren, fünf Mal so häufig Opfer von Kontoübernahmen werden, wie diejenigen, die MFA einsetzen.
>
> Gartner, Inc., Enhance Remote Access Security With Multifactor Authentication and Access Management.
> Ant Allan, Rob Smith, Michael Kelley, 6. Mai 2020

Die Kosten einer Sicherheitsverletzung können Ihr Unternehmen in den Ruin treiben. Die durchschnittlichen Kosten einer Sicherheitsverletzung liegen bei 148 USD pro Datensatz für sensible Daten, was bei einer durchschnittlichen Sicherheitsverletzung mit 9.350 Datensätzen 1,38 Millionen USD entspricht. Die beinhaltet nicht die indirekten Kosten wie geschädigter Unternehmensruf, Verlust des Kundenvertrauens und Ausfallzeiten.

Die gute Nachricht ist, dass Sie Ihr Cyberrisiko problemlos reduzieren und Ihre Sicherheitsinvestitionen gezielt einsetzen können. Es kostet weniger als eine Tasse Kaffee, jedem Mitarbeiter monatlich MFA-Schutz bereitzustellen. Eliminieren Sie das Hauptrisiko für Ihr Unternehmen mit AuthPoint.

Möchten Sie dies testen? Gehen Sie zu watchguard.com/TryAuthPoint oder kontaktieren Sie einen unserer dedizierten Spezialisten, um eine kostenlose 30-tägige Testversion zu erhalten.

1 https://breachalarm.com/
2 https://www.statista.com/statistics/763091/us-use-of-same-online- passwords/
3 https://www.techspot.com/news/77864-worst-passwords-2018-revealed-123456-retains- top-spot.html

DIE 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.

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.

Sicheres, cloud-verwaltetes 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.

Endpoint-Security

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 WatchGuard EPDR 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.

Mehr erfahren

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

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 Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von mehr als 250.000 Kunden. 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 Pazifikraum. Weitere Informationen finden Sie unter **WatchGuard.com/de**.