

AUTHPOINT

Reduzieren Sie Ihr Risiko dank leistungsstarker, benutzerfreundlicher Multifaktor-Authentifizierung



PASSWÖRTER REICHEN NICHT AUS

Jeden Tag verwenden Cyberkriminelle gestohlene Anmeldedaten, um auf Systeme zuzugreifen, diese zu infizieren oder Daten zu stehlen. Um diesem Trend entgegenzuwirken, muss für die Authentifizierung neben einem einfachen Benutzernamen und einem Passwort, ein zusätzlicher Identitätsnachweis angegeben werden. Außerdem sollte diese Strategie von sämtlichen Unternehmen – unabhängig von ihrer Größe – verfolgt werden.

MULTIFAKTOR-AUTHENTIFIZIERUNG WEHRT BETRÜGER AB

Mit WatchGuard AuthPoint® können Sie diese Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach und zum richtigen Zeitpunkt schließen. Die mobile AuthPoint-App verschafft - dank einfacher Push-Benachrichtigungen – eine umfassende Transparenz der Anmeldeversuche, sodass Benutzer den Zugriff direkt über ihr Smartphone gewähren oder blockieren können. Beim einzigartigen Ansatz von WatchGuard wird die „DNA des Mobiltelefons“ als weiterer Identifizierungsfaktor genutzt. Auf diese Weise wird sichergestellt, dass nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen erhält.

INTUITIVE CLOUD-VERWALTUNG

Aufgrund der komplexen Integration und der aufwändigen lokalen Verwaltung war Multifaktor-Authentifizierung für einige Unternehmen lange Zeit keine Option. Die Implementierung war ohne einen großen Stamm an IT-Mitarbeitern und ohne hohe Vorabinvestitionen nicht zu stemmen. Bei WatchGuard AuthPoint hingegen handelt es sich um einen Cloud-Dienst, sodass keine teure Hardware bereitgestellt werden muss und die Lösung ortsunabhängig über die intuitive Schnittstelle von WatchGuard Cloud verwaltet werden kann. Darüber hinaus bietet unsere umfassende Infrastruktur Dutzende Integrationen mit Drittanbieteranwendungen. Auf diese Weise lässt sich sicherstellen, dass Multifaktor-Authentifizierung weitgehend für den Zugriff auf vertrauliche Cloudanwendungen, Webdienste, VPNs und Netzwerke angewendet wird. AuthPoint-User müssen sich nur einmal anmelden, um auf mehrere Anwendungen zuzugreifen und haben außerdem die Möglichkeit, Authentifikatoren von Drittanbietern, wie zum Beispiel von Facebook oder Google Authenticator, zu der benutzerfreundlichen mobilen App hinzuzufügen.

“ *AuthPoint ist großartig, funktioniert hervorragend und ist benutzerfreundlich – bevor ich es getestet habe, war ich skeptisch.* ”

Don Gulling, President & CEO, Verteks Consulting

DREI MÖGLICHKEITEN ZUR APP-AUTHENTIFIZIERUNG



Push-basierte Authentifizierung

Sichere Authentifizierung mit One-Touch Genehmigung. Sie sehen wer sich authentifizieren möchte inkl. seines Standorts und Sie können nicht autorisierten Zugriff auf Ihre Ressourcen blockieren.

QR-Code-basierte Authentifizierung

Mit der Smartphone-Kamera können Sie einen eindeutigen, verschlüsselten QR-Code mit einer Challenge einlesen, die nur von der App gelesen werden kann. Die passende Antwort für den Abschluss der Authentifizierung ist bereits enthalten.



Zeitbasiertes Einmalkennwort (One-Time Password, OTP)

Ein dynamisches, zeitbasiertes Einmalkennwort wird abgerufen und - wie angezeigt- bei der Anmeldung eingegeben.

FUNKTIONEN UND VORTEILE

- Online-Authentifizierung (Push) und Offline-Authentifizierung (QR-Code und OTP)
- Cloud-Service mit geringen Betriebskosten (TCO)
- Überprüfung der „DNA“ des Smartphones für einen starken Identitätsabgleich
- Einfache mobile App mit vollem Funktionsumfang in 13 Sprachen
- VPN-, Cloud- und PC-Anmeldeschutz inbegriffen
- Portal für Web-Single Sign-On (SSO)
- Schutz von VPNs, Cloud-Apps und Webdiensten einfach gemacht, mithilfe von Anleitungen zur Integration
- Konfiguration von „Safe Locations“ für komfortable MFA-Bypass in

Mobile AuthPoint-App

AUTHENTIFIZIERUNGSFUNKTIONEN

Push-basierte Authentifizierung (online)

QR-Code-basierte Authentifizierung (offline)

Zeitbasiertes Einmalkennwort (offline)

SICHERHEITSFUNKTIONEN

DNA des Smartphones

Onlineaktivierung mit Erstellung von dynamischen Schlüsseln

Authentifikatorzugriff über PIN, Fingerabdruck und Gesichtserkennung (iPhone X)

Self-Service: Sichere Migration des Authentifikators von einem Smartphone zum Nächsten

Jailbreak und Root-Detection

PRAKTISCHE FUNKTIONEN

Unterstützung mehrerer Tokens

Unterstützung für Hardware-Token von Drittanbietern

Unterstützung für Social-Media-Token von Drittanbietern

Token-Name und -Bild (benutzerdefiniert)

UNTERSTÜTZTE PLATTFORMEN

Android v4.4 oder höher

iOS v9.0 oder höher

UNTERSTÜTZTE SPRACHEN

Englisch, Spanisch, Portugiesisch (Brasilien und Portugal), Deutsch, Niederländisch, Französisch, Italienisch, Japanisch, Chinesisch (vereinfacht und traditionell), Koreanisch, Thai

STANDARDS

OATH Time-Based One-Time Password Algorithm (TOTP) – RFC 6238

OATH Challenge-Response Algorithms (OCRA) – RFC 6287

OATH Dynamic Symmetric Key Provisioning Protocol (DSKPP) – RFC 6063

AuthPoint-Dienst

UNTERSTÜTZTE ANWENDUNGSFÄLLE

Cloud-basierte Authentifizierung mit Web-SSO

Remote-Zugriff, Remote-Desktop und VPN-Authentifizierung

Windows-Anmeldeschutz (online/offline)

macOS-Anmeldeschutz (online/offline)

Linux-Anmeldeschutz

VERWALTUNGSFUNKTIONEN

WatchGuard Cloud Plattform

Active Directory- sowie LDAP-Benutzersynchronisierung und -authentifizierung

Dashboard mit Monitoring- und Reporting-Widgets

Zugriffsrichtlinie pro Benutzergruppe

Konfigurierbare Authentifizierungsressourcen

Einfache Bereitstellung mit Integrationsanleitung

Protokolle und Berichte

Konfiguration von Safe Locations

AUTHPOINT-GATEWAY

Sichere ausgehende Verbindung vom Netzwerk zur WatchGuard Cloud

MS-AD- und LDAP-Synchronisierung

RADIUS-Server

AUTHPOINT-AGENTEN

Windows-Anmeldung

macOS-Anmeldung

ADFS

RD Web

STANDARDS

RADIUS

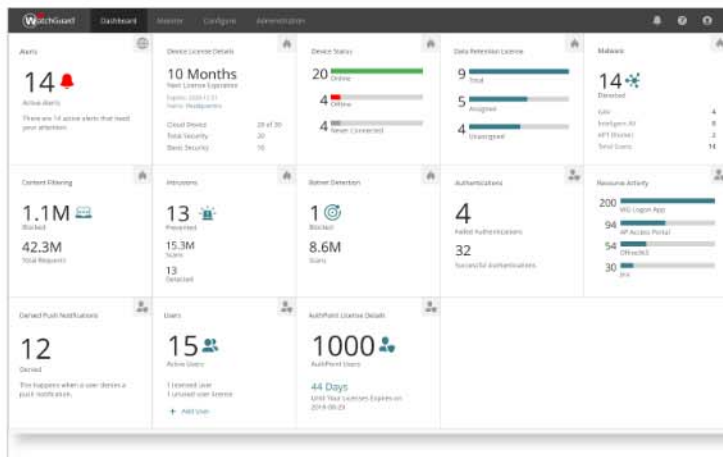
SAML 2.0 IdP

INTEGRATIONEN (EINE VOLLSTÄNDIGE LISTE FINDEN SIE AUF DER WATCHGUARD-WEBSITE)

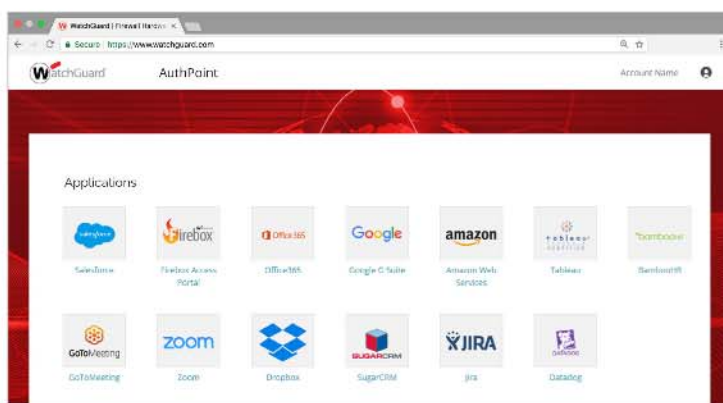
Microsoft Office 365, G-Suite, WatchGuard Firebox, Dropbox, Go-to-Meeting, Open VPN



Mobile AuthPoint-App



WatchGuard Cloud-Management



Integrationen und SSO

DAS WATCHGUARD-SICHERHEITSPORTFOLIO



Netzwerksicherheit



Sicheres WLAN



Multifaktor-Authentifizierung

Weitere Informationen erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter www.watchguard.de.

Dieses Dokument gilt ohne ausdrückliche oder implizierte Gewähr. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. © 2019 WatchGuard Technologies, Inc.. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox und AuthPoint sind Marken bzw. eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenummer. WGCE67094_071119