Warum Sie WatchGuard Identity Security kaufen sollten

Die AuthPoint-Lösungen zum Schutz der Identität umfassen Multifaktor-Authentifizierung (MFA), erweiterte Funktionen zur Passwortgenerierung und sichere Passwort-Tresore. Mit den Tools von AuthPoint bleiben Unternehmen in einer zunehmend digitalen Welt sicher. Darüber hinaus sind Unternehmen dank unserer Dark Web Monitoring-Funktion einen Schritt voraus, da sie kompromittierte Anmeldeinformationen erkennen, bevor diese böswillig eingesetzt werden können.

Wichtige AuthPoint-Funktionen und -Vorteile zum Schutz der Identität

Mit erweiterten Funktionen zur Passwortgenerierung und für das Dark Web Monitoring schützen Sie die Anmeldeinformationen des Unternehmens

Prämierter MFA-Service

AuthPoint MFA wird über WatchGuard Cloud bereitgestellt und erleichtert Benutzern die Authentifizierung mit Offline- und Online-Verifizierungsmethoden und Zugriffsrichtlinien für Endpoints, VPNs und Webanwendungen. Ein effizienter und sicherer Zugriff auf Cloud-Ressourcen ist auch über SSO-Anwendungsportale (Single Sign-On) möglich.

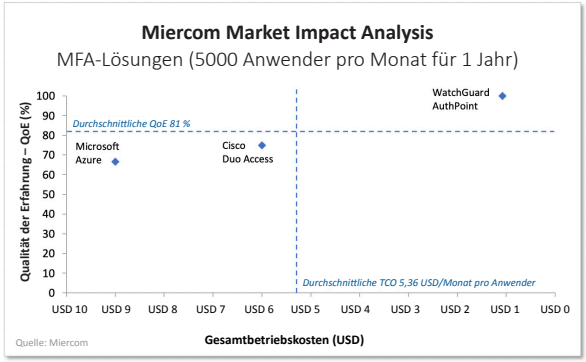
Dark Web Monitoring-Service

Der Dark Web Monitoring-Service von AuthPoint benachrichtigt Kunden proaktiv, wenn kompromittierte Anmeldeinformationen von bis zu drei überwachten Domänen in neu erworbenen Datenbanken für Anmeldeinformationen gefunden werden. An betroffene Administratoren und Endbenutzer werden Warnmeldungen gesendet, damit diese schnell und vor einer Kontoübernahme neue Passwörter generieren können.

Password Manager

AuthPoint Password Manager wurde speziell für geschäftliche Anwendungsfälle entwickelt und bietet Unternehmen einen höheren Standard mit sicheren Passwörtern. Mit dem Password Manager generierte Passwörter müssen nicht von den Benutzern auswendig gelernt werden. Dadurch kann die Anzahl der Passwortrücksetzungen reduzieren werden. Zusätzlich bietet der Password Manager folgende Vorteile:

- **Tresor für geschäftliche Passwörter:** Fügen Sie Anmeldeinformationen hinzu und generieren Sie sichere Passwörter für häufig verwendete Arbeitsplatzanwendungen, bei denen SSO nicht aktiviert ist. Außerdem können Administratoren Anmeldeinformationen für die gemeinsame Nutzung von IT-Anwendungen und -Tools freigeben.
- **Tresor für private Passwörter:** Fügen Sie Anmeldeinformationen hinzu und generieren Sie sichere Passwörter für persönliche Apps und soziale Medien. Wenn der Mitarbeiter die Organisation verlässt, können diese persönlichen Anmeldeinformationen exportiert und in einem anderen Passwort-Manager genutzt werden.



Die Quadranten basieren auf den Durchschnittswerten. WatchGuard befand sich im oberen rechten Quadranten – die Lösung besaß die höchste QoE unter den konkurrierenden Anbietern, und zwar zu den niedrigsten Kosten. Cisco und Microsoft bieten nicht annähernd den gleichen Funktionsumfang, eine ähnliche Benutzerfreundlichkeit oder eine vergleichbar intuitive Oberfläche wie WatchGuard.

Warum Unternehmen sich für AuthPoint MFA entscheiden

Sicherheit bei hybridem Arbeiten leicht gemacht

Vereinfachen Sie die Passwortverwendung mit SSO-Konfigurationen (Single Sign-On), die Remote-Arbeit mit sicherer Anmeldung und sicherem Zugriff auf Anwendungen ermöglichen.

Nahtlose Benutzererfahrung

Einer unabhängigen Produktvalidierung zufolge ist AuthPoint dank seiner intuitiven Benutzeroberfläche, der hilfreichen Anleitungen und Ein-Klick-Einrichtung die erste Wahl für Erstanwender und damit empfehlenswerter als andere Lösungen auf dem Markt.

Mobile DNA für sichere Migration

Die MFA-Lösung von WatchGuard enthält eine DNA-Funktion für mobile Geräte, die automatisch die Übereinstimmung mit dem Telefon des autorisierten Benutzers prüft, bevor der Zugriff gewährt wird. Angreifer, die das Gerät eines Benutzers klonen, um auf geschützte Systeme zuzugreifen, werden sofort blockiert.

Hoher Wert und hohe Rentabilität

Im Vergleich zu anderen Lösungen bietet WatchGuard eine Vielzahl nativer Funktionen, Hunderte Integrationen und einen dedizierten Kundensupport – und das alles zu einem Festpreis pro Benutzer und Monat.

Einführung von Zero-Trust mit Authentifizierungsrichtlinien

Die adaptiven Richtlinien und Kontrollen von AuthPoint ermöglichen ein einheitliches Zugriffsmanagement und sind damit ein wichtiger Schritt zur Einführung von Zero-Trust-Sicherheit.

Wichtige Funktionen zum Schutz der Identität

Mobile Authenticator-App von AuthPoint

AUTHENTIFIZIERUNGSARTEN
Push-Benachrichtigung mit Phishing-Schalter (Online-Modus)
QR-Code-Generator (Offline-Modus)
Zeitbasierte Einmalpasswörter (Offline-Modus)
SICHERHEITSFUNKTIONEN
Jailbreak und Root-Detection
DNA des Mobilgeräts/SIM-Wechselschutz
Onlineaktivierung mit Erstellung von dynamischen Schlüsseln
App-Schutz: PIN, Fingerabdruck und Gesichtserkennung
Self-Service, sichere Migration zu einem anderen Gerät
Unterstützung mehrerer Token, auch von Drittanbietern
Anpassung von Token-Name und -Symbol
UNTERSTÜTZTE PLATTFORMEN
Android v7.0 oder höher
iOS v12.5.7 oder höher

AuthPoint-Cloud-Management

MANAGEMENTFUNKTIONEN
Administration, Konfiguration und Management mit WatchGuard Cloud
Konfigurierbare Authentifizierungsressourcen
Anpassbare Authentifizierungs- und Risikorichtlinien (Netzwerk, Zeit, Geofence und Geokinetik)
Dark Web Scan von bis zu 3 Domains
Dark Web Monitoring für Anmeldedaten für bis zu 3 Domains pro Lizenz
Dashboard-Widgets für Authentifizierungen, Anwender, Geräte und Abonnements
Einfache Bereitstellung mit Integrationsanleitungen und Assistenten
Synchronisierung mit Active Directory, Azure AD und LDAP
Anwenderübernahme für Service Provider
AUTHPOINT GATEWAY
Sichere ausgehende Verbindung vom Netzwerk zur WatchGuard Cloud
Active Directory- und LDAP-Synchronisierung
RADIUS-Server

AUTHPOINT-AGENTEN UND -INSTALLATIONSPROGRAMME
Anmeldung bei macOS El Capitan (10.11) oder höher
Anmeldung bei Windows v8.1 oder höher
Windows Hello for Business-Anmeldung
Active Directory Federation Server 2012 und höher (SSO)
Anmeldung bei Windows Server 2012 und höher
Windows Remote Desktop Web Access
WatchGuard AuthPoint Gateway Agent
HARDWARE-TOKEN
WatchGuard-Hardware-Token ohne Seed-Offenlegung
TOTP-Hardware-Token von Drittanbietern

UNTERSTÜTZTE 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
RADIUS-Protokoll (IETF)
SAML 2.0-Profil (OASIS)
Argon 2id (Open Source)

AUTHPOINT-INTEGRATIONEN MFA mit Single Sign-On
SAAS: Atlassian, BlueJeans, Box, Citrix, Confluence, Dropbox, Evernote, Github, Google Workspace, Go-to-Meeting, Jira, Lucid Charts, Microsoft 365, Salesforce, ServiceNow, Slack, Tableau, Zoom, WebEx und mehr
IAAS: Adobe Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce Cloud, Oracle Cloud und mehr
Sicherheit und Management: Akamai, BMC, Cisco, ConnectWise, CyberArk Fortinet, ITGlue, JAMF, ManageEngine, MobileIron, PagerDuty, Thycotic, VMware, WatchGuard Firebox, WatchGuard VPN und mehr

Verlassen Sie sich nicht nur auf das, was wir sagen.

TrustRadius

„Eine zuverlässige und kostengünstige 2-Faktor-Authentifizierung für unsere Kunden. Wird hauptsächlich für den MFA-VPN-Zugriff für authentifizierte Benutzer verwendet, die remote arbeiten möchten. Vor dem Umstieg auf WatchGuard AuthPoint hatten wir keine gute Lösung für alle unsere Kunden, die mittels MFA eine Verbindung zu einem VPN herstellen."

– Robbie Matthew, Senior Network Engineer
Invision Technologies, LLC (Telekommunikation, 51-200 Mitarbeiter)

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ: +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.