



# AuthPoint Identity Security

Besonders einfach. Besonders sicher.

Ein einziger kompromittierter Berechtigungsnachweis genügt, um einer Organisation ernsthaft zu schaden oder sie ganz lahmzulegen. Daher muss Identitätssicherheit als vorderste Verteidigungslinie gegen Cyber-Angriffe fungieren.

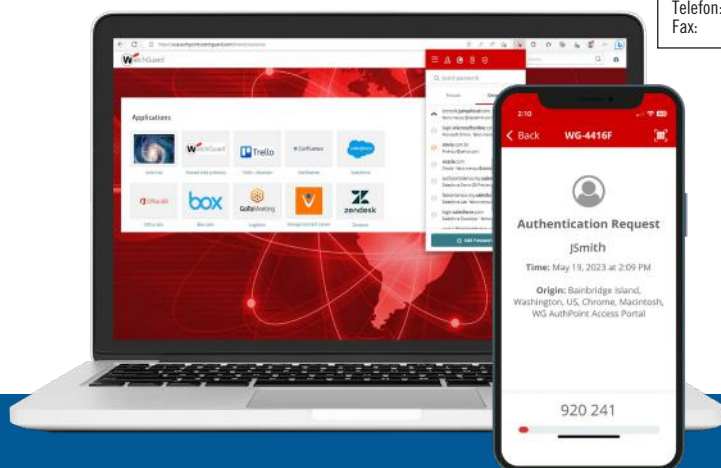
AuthPoint Identity Security bietet die Sicherheit, die Sie brauchen, um Identitäten, Ressourcen, Konten und Informationen zu schützen. Statten Sie Ihr Unternehmen mit benutzerfreundlichen, kostengünstigen und umfassenden Lösungen zur Verwaltung von Anmeldedaten und Multi-Faktor-Authentifizierung aus, damit Sie sicher und sorgenfrei arbeiten können. Erfüllen Sie zudem die Anforderungen für Sicherheits-Frameworks, Compliance und Cyber-Versicherungen im Zusammenhang mit Anwenderauthentifizierung und Zugriffskontrolle.

- Ermöglichen Sie den sicheren Fernzugriff mit virtuellen privaten Netzwerken (VPNs).
- Bieten Sie Mitarbeitern eine nahtlose Erfahrung mit benutzerfreundlicher Sicherheitstechnologie.
- Halten Sie gesetzliche Vorschriften ein und erfüllen Sie die Anforderungen für Cyber-Versicherungen.

**INNEO**<sup>®</sup> Händlerinformation  
**That's IT.**

INNEO Solutions GmbH · inneo@inneo.com · www.inneo.com

Deutschland: IT-Campus 1 73479 Ellwangen	Schweiz: Ruchstuckstrasse 21 CH-8306 Brüttisellen
Telefon: +49 (0) 7961 890-0	Telefon: +41 (0) 44 805 1010
Fax: +49 (0) 7961 890-177	Fax: +41 (0) 44 805 1011



*„AuthPoint hält, was MFA verspricht. Die App reduziert das mit schwachen Passwörtern verbundene Geschäftsrisiko, 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

## Große Herausforderungen von Unternehmen in Bezug auf Identitäten Ihrer Mitarbeiter



82 %

der Datenschutzverletzungen gehen auf den Faktor Mensch zurück. Sie sind damit die häufigste Ursache.



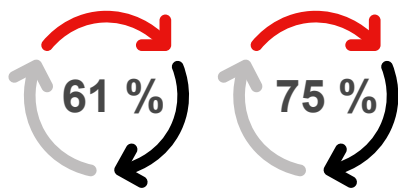
27

Passwörter muss sich ein durchschnittlicher Mitarbeiter merken



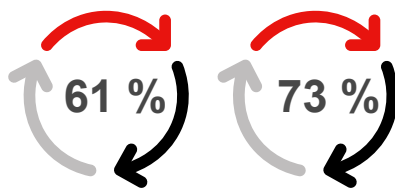
55 %

der Unternehmen unterstützen weiterhin Hybrid-/Remote-Arbeitsmodelle



Großunternehmen vs. KMU

der Datensicherheitsverletzungen hingen mit gestohlenen Anmeldedaten zusammen.



Arbeitsplatz vs. Privat

Wiederverwendung von Passwörtern in verschiedenen Anwendungen und Diensten



der Unternehmen planen, das Sicherheitsmanagement auszulagern und die Authentifizierungs-/Zugriffssteuerung zu intensivieren

## AuthPoint-Lösungen zum Schutz der Identität

*Mindern Sie die Risiken in Verbindung mit großflächigen Angriffen auf Mitarbeiter-Anmeldedaten*

### Multifaktor-Authentifizierung (MFA): Einführung einer konsistenten Benutzerverifizierung

AuthPoint MFA hält der Passwortmüdigkeit stand. So können effizientere Authentifizierungsmaßnahmen mit Funktionen wie dem Phishing Toggle angewendet werden, um eine negative Benutzererfahrung zu verhindern. Unser schnelles, einfach zu implementierendes VPN und der Fernzugriff sorgen für sicheren Zugang bei minimalem Aufwand. Mit den verfügbaren Offline- und Online-Authentifizierungsmethoden können Sie ein stets hohes Sicherheitsniveau bei Ihrem System mühelos sicherstellen. Darüber hinaus ermöglichen das umfassende Integrations-Ökosystem und der SAML-Standard vollständigen Zugriff. So können Unternehmen die Zugriffsrechte für Benutzer schnell und effektiv steuern.



AuthPoint MFA

Nur Multifaktor-Authentifizierung

### Corporate Password Manager: Passwortsicherheit und Benutzererfahrung verbessern

Der Corporate Password Manager gibt Unternehmen mehr Kontrolle über die Qualität von Passwörtern, reduziert die Anzahl erforderlicher Passwörterücksetzungen und entschärft Probleme im Zusammenhang mit wiederverwendeten, weitergegebenen oder gestohlenen Passwörtern. Mit einem Passwortmanager erstellte Passwörter sind praktisch unmöglich zu knacken, aber viele bieten nicht die Funktionen, die Unternehmen benötigen. Wenn Benutzer auf ihre Anwendungen oder Systeme zugreifen müssen, können sie mit dem Corporate Password Manager von WatchGuard über die AuthPoint-App und/oder die Browser-Erweiterung ihre geschäftlichen, persönlichen und gemeinsamen Tresor-Passwörter abrufen. Dadurch können Unternehmen Nicht-SAML-Cloud-Anwendungen zum Web-SSO-Portal hinzufügen, um eine zuverlässigere Authentifizierung und ein reibungsloses SSO-Erlebnis zu gewährleisten.



AuthPoint Total Identity Security

Multi-Faktor-Authentifizierung PLUS Anmeldedatenverwaltung

### Dark Web Monitoring: Werden Sie aktiv, wenn Anmeldedaten im Darknet landen

Der Dark Web Monitor ist ein proaktiver Dienst, der Kunden benachrichtigt, wenn kompromittierte Anmeldedaten von überwachten Domains in einer neu erworbenen Datenbank für Anmeldedaten gefunden werden, die in unserem Dienst veröffentlicht wird. Benachrichtigungen können sowohl an die von der Sicherheitsverletzung betroffenen Benutzer als auch an die Administratoren gesendet werden, damit die Benutzer ihr Passwort proaktiv ändern können. Mit einer einzigen Lizenz können bis zu drei Domains überwacht werden.

## Hacker brechen nicht ein – sie melden sich an

*AuthPoint ermöglicht eine anpassbare Zugriffsumgebung mit mehr Produktivität und weniger Ausgaben*



### Risiko-Framework auf Basis von Zero-Trust

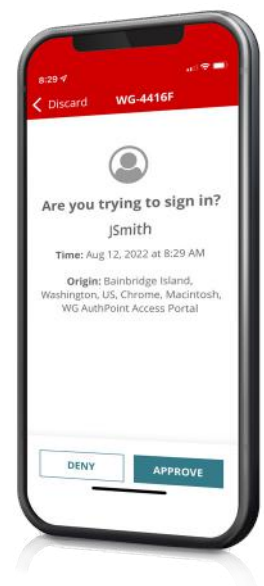
Die Einführung von Zero-Trust funktioniert nur mit Identitätssicherheit. Unsere risikobasierten Zugangsrichtlinien stellen sicher, dass nur der richtige Nutzer zur richtigen Zeit Zugang erhält. AuthPoint bietet anpassbare Authentifizierungs- und Risikoricthlinien ohne zusätzliche Kosten, einschließlich Netzwerk-, Zeit-, Geofence- und Geokinetics-Funktionen.

### Umfassende Abdeckung mit Single Sign-on (SSO)

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 Passwortmüdigkeit mit sich bringt. Zudem wird das Risiko von Sicherheitsschwachstellen aufgrund schwacher Passwörter gesenkt und Kosten werden verringert, die mit dem Zurücksetzen von Passwörtern einhergehen.

### Geringe 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. Ganz gleich, ob Sie nur MFA oder Total Identity Security anwenden – AuthPoint bietet ein umfassendes Preismodell pro Anwender und Monat, damit Unternehmen ihre Maßnahmen zur Identitätssicherheit ohne Extrakosten vollständig umsetzen können.

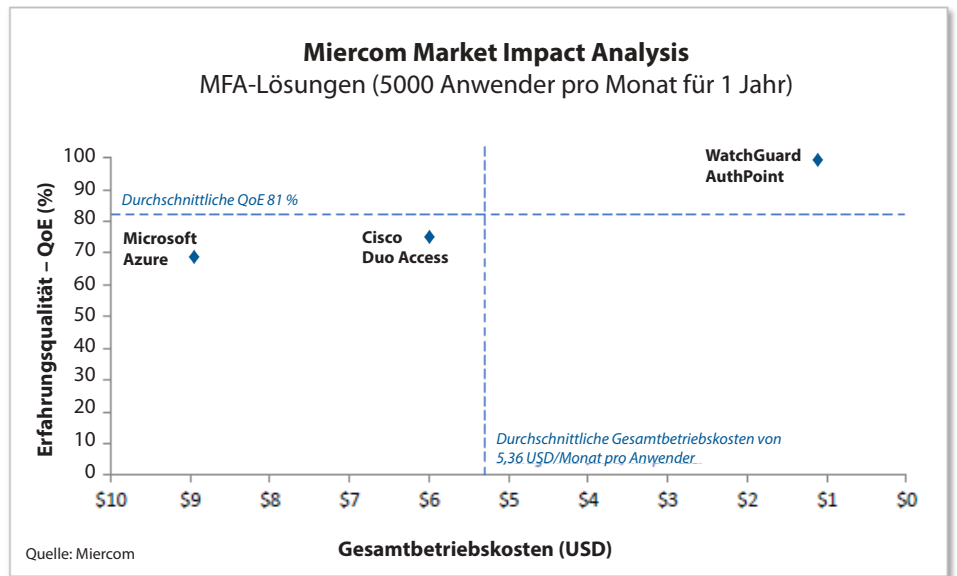


## Miercom – externe technische Validierung

Miercom, ein IT-Labor, das Validierungen durch Dritte durchführt, hat der AuthPoint MFA-Lösung von WatchGuard das Zertifikat „Performance Verified“ verliehen. Im Rahmen dieser Bewertung hat Miercom die Benutzerfreundlichkeit und Leistungsfähigkeit von AuthPoint im Vergleich mit Cisco Duo und Azure MFA getestet.

## Hoher Wert und hohe Rentabilität als Wettbewerbsvorteil

WatchGuard hat mit seiner herausragenden Erfahrungsqualität den höchsten Wert nachgewiesen. Im Vergleich zu anderen Lösungen bietet WatchGuard mit dem einmaligen Kauf eine Vielzahl von nativen Funktionen. Andere Lösungen sind komplexer und kostenintensiver, da zusätzliche Abonnements erforderlich sind.



Die Quadranten basieren auf den Durchschnittswerten. WatchGuard befindet 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.

## DAS WATCHGUARD PORTFOLIO



### Netzwerksicherheit

WatchGuard bietet eine breite Palette an Netzwerksicherheitslösungen, von Tabletops und 1-HE-Rackmount-Appliances bis hin zu cloudbasierten und virtuellen Firewalls. Unsere Firebox® Appliances bieten wichtige Sicherheitsdienste, von Standard-IPS, URL-Filterung, Gateway-AV, Anwendungskontrolle und Antispam bis hin zu erweiterten Schutzfunktionen wie Datei-Sandboxing, DNS-Filterung und mehr. Dank der leistungsstarken Deep Packet Inspection (DPI) können Sie alle unsere Sicherheitsdienste gegen Angreifer einsetzen, die versuchen, sich hinter verschlüsselten Kanälen wie HTTPS zu verstecken. Außerdem bietet jede Firebox standardmäßig SD-WAN, was die Ausfallsicherheit und Leistung des Netzwerks erhöht.



### Identitätssicherheit

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. AuthPoint bietet ebenfalls eine optimierte Benutzererfahrung mit Online- und Offline-Authentifizierungsmethoden sowie ein Webanwendungsportal für einfachen Single Sign-On-Zugriff.



### Sicheres, cloudveraltetes WLAN

Die sicheren, cloudverwalteten WLAN-Lösungen von WatchGuard bieten einen sicheren, geschützten Rahmen für WLAN-Umgebungen, ohne dass Sie sich um die Verwaltung kümmern müssen. Gleichzeitig werden die Kosten erheblich gesenkt. Von Heimbüros bis hin zu großflächigen Firmengeländen stellt WatchGuard die WLAN 6-Technologie mit sicherer WPA3-Verschlüsselung bereit. Dank WatchGuard Cloud sind WLAN-Netzwerkkonfiguration und Richtlinienverwaltung, Zero-Touch-Bereitstellung, benutzerdefinierte Captive Portals, VPN-Konfiguration, umfangreiche Interaktionstools, Einblicke in Geschäftsanalysen und Upgrades nur einen Klick entfernt.



### Endpoint-Sicherheit

Mit den Lösungen von WatchGuard Endpoint Security schützen Sie Ihre Geräte vor Cyber-Angriffen. WatchGuard EPDR und Advanced EPDR, unsere erstklassigen KI-gestützten Endpoint-Lösungen, verbessern Ihre Sicherheitslage durch die nahtlose Integration von Endpoint Protection (EPP) mit Funktionen für Detection and Response (EDR) und unseren Zero-Trust Application und Threat Hunting Services. Diese sind alle vollständig in die WatchGuard Cloud und ThreatSync integriert und bieten wertvolle Einblicke und Erkenntnisse, wobei sie gleichzeitig die produktübergreifende Erkennung und Reaktion (XDR) stützen.

## Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. WatchGuards Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Network Security und Intelligence fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter [WatchGuard.de](http://WatchGuard.de).