AuthPoint Identity Security

AuthPoint Identity Security solutions include our award-winning multi-factor authentication (MFA). Plus, it adds a corporate password manager and credential monitoring to help mitigate the risks associated with widespread workforce credential attacks.

MFA

Mobile Authenticator App for iOS & Android

Corporate Password Manager

Auto-fill credentials with browser extensions for Chrome, Edge, Safari, & Firefox

Dark Web Monitoring

Dark web credential monitoring for up to three domains per license

AuthPoint Integrations

Web application portal enabled with single sign-on access

Cloud Management

Zero trust risk policies based on location, time, and device DNA

Mobile App

Push notification with phishing toggle and online/ offline modes available

AUTHPOINT MOBILE AUTHENTICATOR APP	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
AUTHENTICATOR TYPES		
Push Notification with Phishing Toggle (online mode)	●	●
QR Code Generator (offline mode)	●	●
Time-based One Time Passcode (offline mode)	●	●
SECURITY FEATURES		
Jailbreak and Root Detection	●	●
Mobile Device DNA / SIM Swap Protection	●	●
Online activation with Dynamic Key Generation	●	●
App Protection: PIN, fingerprint, and face recognition	●	●
Self-service, secure migration to another device	●	●
Third-party and multi-token support	●	●
Token name and icon customization	●	●
CORPORATE PASSWORD MANAGER		
Corporate Vault and Private Vault		●
Shared vaults for IT managers and MSPs		●
Credential Health Monitoring and Alerts		●
Advanced Complex Password Generation		●
SUPPORTED PLATFORMS		
Android v7.0 or higher	●	●
iOS v12.5.7 or higher	●	●

AUTHPOINT CLOUD MANAGEMENT	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
MANAGEMENT FEATURES		
Administration, configuration, and management with WatchGuard Cloud	●	●
Audit, logging, and reporting	●	●
Configurable authentication resources	●	●
Customizable authentication and risk policies (network, time, geofence and geokinetics)	●	●
Dark Web Scan of up to 3 domains	●	●

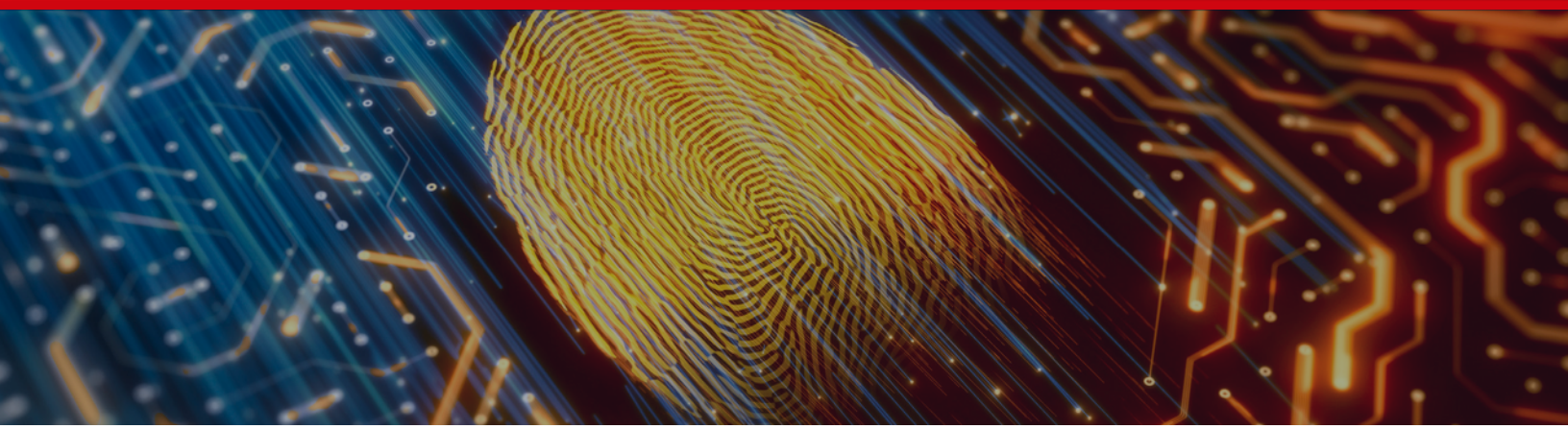
● *AuthPoint Total Identity Security Only Feature*

Dark Web Credential Monitoring of up to 3 domains per license		●
Dashboard widgets for authentications, users, devices, and subscriptions	●	●
Easy deployment with integration guides and wizards	●	●
Synchronization with Active Directory, Azure AD and LDAP	●	●
User inheritance for service providers	●	●
AUTHPOINT GATEWAY		
Secure outbound connection from network to WatchGuard	●	●
Cloud Active Directory and LDAP synchronization	●	●
RADIUS Server	●	●
AUTHPOINT AGENTS & INSTALLERS		
macOS El Capitan (10.11) or higher logon	●	●
Windows v8.1 or higher logon	●	●
Windows Hello for Business logon	●	●
Active Directory Federation Server 2012 and above	●	●
(SSO) Windows Server 2012 and above logon	●	●
Windows Remote Desktop Web Access	●	●
WatchGuard AuthPoint Gateway Agent	●	
HARDWARE TOKEN		
WatchGuard hardware token with no seed exposure	●	●
Third party TOTP hardware tokens	●	●
BROWSER SUPPORT		
Password Manager Browsers Extension: Google Chrome, Microsoft Edge, Firefox, & Safari		●
Password Manager: Auto-fill credentials for websites		●
Password Manager: Forms-based authentication with single sign-on (SSO)		●

AUTHPOINT INTEGRATIONS MFA with Single Sign-On	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
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 and more...	●	●
IAAS: Adobe Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce Cloud, Oracle Cloud and more...	●	●
Security & Management: Akamai, BMC, Cisco, ConnectWise, CyberArk Fortinet, ITGlue, JAMF, ManageEngine, MobileIron, PagerDuty, Thycotic, VMWare, WatchGuard Firebox, WatchGuard VPN, and more...	●	●

	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
SUPPORTED LANGUAGES		
English, Spanish, Brazilian Portuguese, Portuguese, German, Dutch, French, Italian, Japanese, Simplified Chinese, Traditional Chinese, Korean, Thai		
SUPPORTED 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 Protocol (IETF)	●	●
SAML 2.0 Profile (OASIS)	●	●
Argon 2id (Open Source)		●

● *AuthPoint Total Identity Security Only Feature*



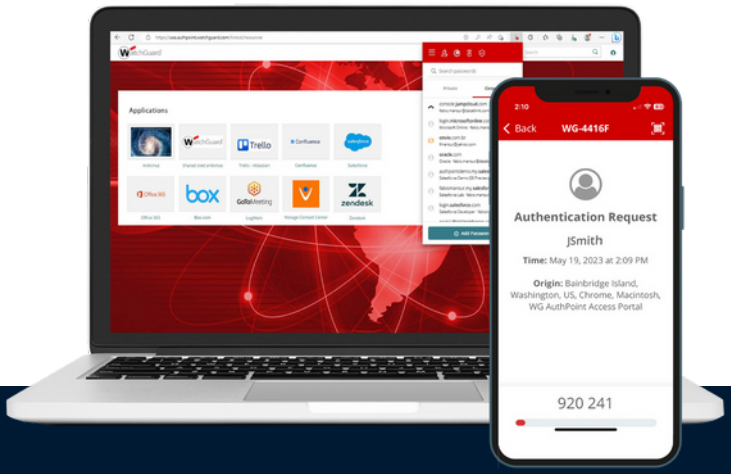
AuthPoint Identity Security

Uniquely Simple. Powerfully Secure.

It takes only one compromised credential to seriously damage or even disable an organization. Identity security needs to be the first line of defense against cyberattacks.

AuthPoint Identity Security provides the security you need to protect identities, assets, accounts, and information. Let your company work confidently and worry-free with easy-to-use, cost-effective, and complete multi-factor authentication and credential management solutions. Plus, meet security frameworks, compliance, and cyber insurance requirements related to user authentication and access control.

- Enable secure remote access with virtual private networks (VPNs)
- Provide a seamless experience to employees with simple-to-use security technology
- Achieve regulatory compliance and meet cyber insurance requirements



"AuthPoint delivers on the promise of MFA by limiting the business risk associated with poor passwords without compromising on ease of use for employees and IT staff alike.

Everything in a Cloud service – with no hardware to install and software to maintain... MFA is now considered core protection, and it comes from WatchGuard hassle-free."

Tom Ruffolo

CEO, eSecurity Solutions

OX IT Solutions Ltd

WatchGuard

Identity Security and MFA

Key Challenges Businesses Have With Workforce Identities

82%

Data breaches involved a human element. People play the largest role

27

An average employee has 27 passwords to remember

55%

Businesses will continue to support hybrid/remote work arrangements

61% **75%**

Enterprise vs. SMB
Data breaches involved the use of stolen credentials

61% **73%**

Workplace vs. Personal
Reuse rates of passwords across apps and services

42% **35%**

Businesses plan to outsource security and increase authentication/ access controls

AuthPoint Identity Security Solutions

Mitigate the risks associated with widespread workforce credential attacks

Multi-Factor Authentication (MFA): Establish Consistent User Verification
AuthPoint MFA is designed to be fatigue-resistant, allowing for more efficient authentication measures with features like the phishing toggle that prevent a faulty user experience. Our easy-to-deploy, fast VPN and remote access provide secure pathways with minimal effort. With offline and online authentication methods available, you can easily ensure that your system always has strong security in place. Plus, the broad integrations ecosystem and SAML standard provide full-range access, giving organizations the ability to control user access privileges quickly and effectively.

AuthPoint MFA

Multi-Factor Authentication Only

Corporate Password Manager: Optimize Password Security and User Experience
The Corporate Password Manager gives companies more control over password quality, reduces the need for password resets, and mitigates issues related to reused, shared or stolen passwords. Passwords created with a password manager are virtually impossible to crack, but many don't deliver the features that businesses need. With WatchGuard's Corporate Password Manager, when users need to access their apps or systems, they can retrieve their corporate, personal, and shared vault passwords using the AuthPoint app and/or browser extension. This allows organizations to add non-SAML Cloud applications to the Web SSO Portal for stronger authentication and a smooth SSO experience.

AuthPoint Total Identity Security

Multi-Factor Authentication PLUS Credential Management

Dark Web Monitoring: Take Action When Credentials Land on Darknets
The Dark Web Monitor is a proactive service that notifies customers when compromised credentials from monitored domains are found in a newly acquired credentials database that's published in our service. Notifications can be sent out to users involved in the breach as well as administrators, so users can proactively change their password. Up to three domains can be monitored with a single license.

Hackers Don't Break In – They Log In

AuthPoint Enables an Adaptive Access Environment with More Productivity and Less Spending

Zero Trust Risk Framework

Zero trust adoption cannot happen without identity security. Our risk-based access policies enable access to the right user at the right time. AuthPoint provides customizable authentication and risk policies at no additional cost, including network, time, geofence, and geokinetics capabilities.

Broad Coverage with Single Sign-On (SSO)

AuthPoint's secure single sign-on (SSO) makes it easier for users to access multiple Cloud applications, VPNs and networks with only one set of credentials. This combats the challenges presented by password fatigue and reduces the risk of security vulnerabilities due to weak passwords and costs associated with password resets.

Low Total Cost of Ownership (TCO)

Companies with limited IT staff and security expertise benefit from MFA protection that's easy to deploy and manage from the Cloud. Whether you deploy just MFA or Total Identity Security, AuthPoint offers an all-inclusive price structure per user, per month to allow companies to fully adopt identity security measures without added cost.

OX IT Solutions Ltd

WatchGuard

Identity Security and MFA

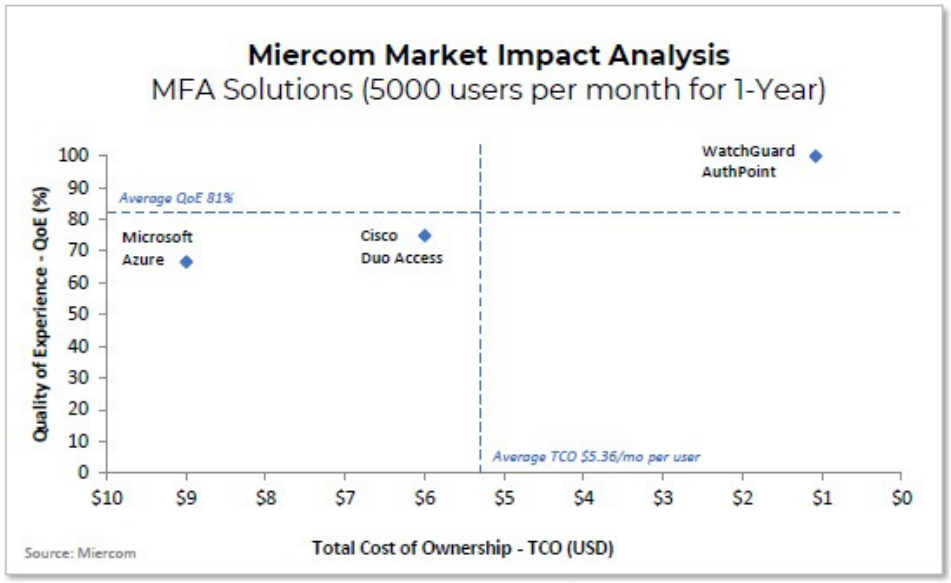
Miercom

Miercom Third-Party Technical Validation

Miercom, an IT lab that provides third-party validation, granted WatchGuard's AuthPoint MFA solution the Performance Verified certification. This assessment tested AuthPoint and validated its usability and performance in comparison with Cisco Duo and Azure MFA.

High Value and ROI Competitive Advantage

WatchGuard showed the highest value with its quality of experience. Compared to other solutions, WatchGuard delivered a rich set of native features with its one-time purchase, while the other solutions have added complexity and cost, requiring the purchase of extra subscriptions.

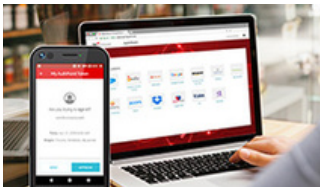


Quadrants are formed based off average values. WatchGuard was in the upper right quadrant, showing it had the highest QoE of competing vendors at the lowest cost. Cisco and Microsoft do not offer nearly the same amount of functionality, ease of use, or intuitive interface as WatchGuard.

THE WATCHGUARD PORTFOLIO

Network Security

WatchGuard offers a wide range of network security solutions, including everything from tabletop and 1U rack- mounted appliances to Cloud and virtual firewalls. Our Firebox® appliances deliver critical security services, from standard IPS, URL filtering, gateway AV, application control, and antispam, to advanced protections such as file sandboxing, DNS filtering, and more. High-performance deep packet inspection (DPI) means you can leverage all our security services against attacks attempting to hide in encrypted channels like HTTPS.



Identity Security

WatchGuard's AuthPoint Identity Security solutions are designed to provide top- rated multi-factor authentication (MFA) and zero trust risk policies for maximum online protection. Enjoy the convenience of a corporate password manager that automatically fills in credentials across browsers like Chrome, Edge, Safari, and Firefox. Leverage our dark web monitoring services to mitigate the risks of widespread workforce credential attacks. AuthPoint also delivers optimized user experience with online and offline authentication methods, along with a web application portal for easy single sign-on access.

Secure Cloud Wi-Fi

WatchGuard's secure, Cloud-managed Wi-Fi solutions provide safe, protected airspace for Wi-Fi environments while eliminating administrative headaches and greatly reducing costs. From home offices to expansive corporate campuses, WatchGuard offers Wi-Fi 6 technology with secure WPA3 encryption. With WatchGuard Cloud, Wi-Fi network configuration and policy administration, zero-touch deployment, customized captive portals, VPN configuration, expansive engagement tools, visibility into business analytics, and upgrades are only a click away.

Endpoint Security

Confidently protect your devices from existing and emerging threats with WatchGuard Endpoint Security solutions. Our AI-powered flagship endpoint security solution, WatchGuard EPDR, can immediately and dramatically improve an organization's security posture by combining endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services. Manage all our endpoint security services via WatchGuard Cloud to gain the visibility, intelligence, and expertise you need to deliver advanced prevention, detection, containment, and response capabilities.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world- class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.