

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 monitoring 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

Key Challenges Businesses Have With Workforce Identities



68%

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

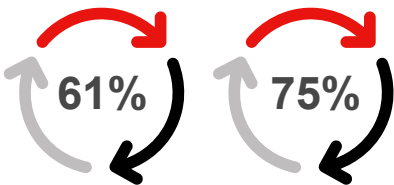
65%

Of stolen credentials are posted for sale in less than one day. Personally identifiable information (PII) is a \$40B business in dark web marketplace



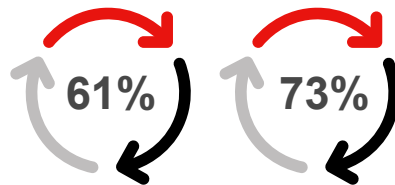
55%

Businesses will continue to support hybrid/remote work arrangements



Enterprise vs. SMB

Data breaches involved the use of stolen credentials



Workplace vs. Personal

Reuse rates of passwords across apps and services



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

Dark Web Monitoring: Take Action When Credentials Land on Darknets

The dark web monitor is a proactive AI-driven service that actively identifies credential information from monitored domains found in breached databases on dark web marketplaces. This advanced threat intelligence offers real-time visibility and notifies customers when credentials have been compromised, which can be swiftly transformed into detection and remediation actions.



AuthPoint Total Identity Security

Multi-Factor Authentication PLUS Credential Monitoring

Mobile DNA: Elevate MFA Protection for Smartphones

AuthPoint MFA protects against SIM swap threats by verifying the user's phone using a mobile device's unique features and encrypted data. This ensures secure access and prevents cloning attempts.

Logon Security: Protect Access on Windows and Mac Devices

AuthPoint software agents can be installed on any machine, regardless of the operating system. Whether you are using macOS, Windows, or Linux, the software integrates seamlessly into existing systems. With both online and offline verification methods available, it ensures secure login processes without sacrificing user convenience.

Hackers Don't Break In – They Log In

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



Zero Trust Risk Framework

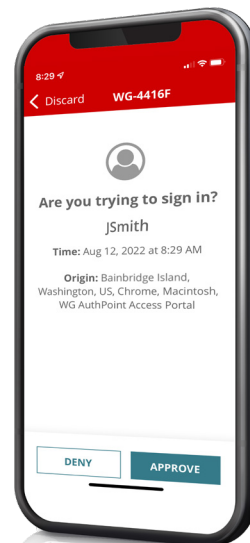
Zero trust adoption cannot happen without identity security. Our risk-based access policies enable access to the right user at the right time. AuthPoint provides customizable authentication and risk policies at no additional cost, including network, time, geofence, and geokinetics capabilities.

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.

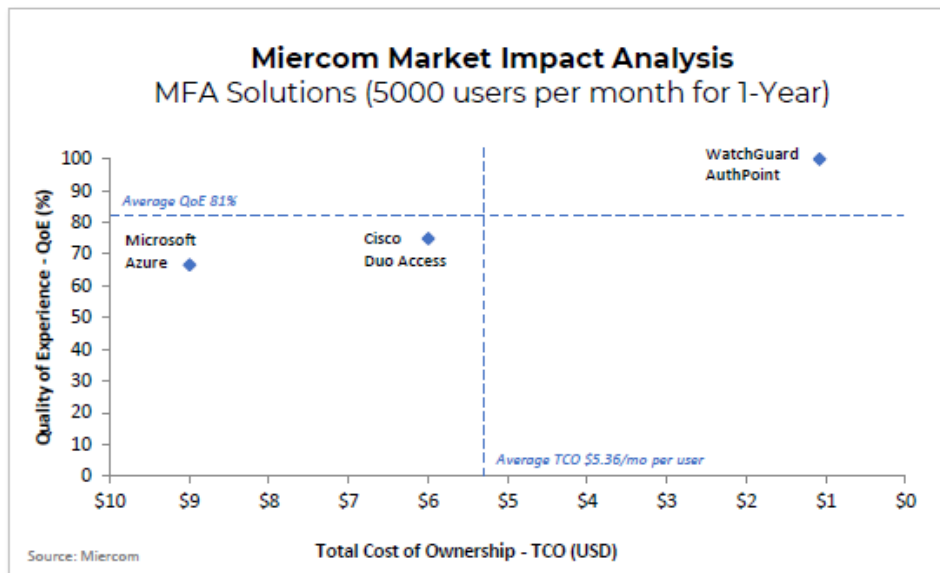


Miercom Third-Party Technical Validation

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.

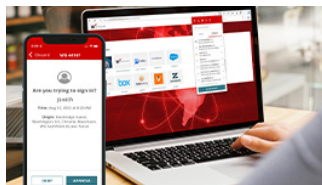
Quadrants are formed based off average values. WatchGuard was in the upper right quadrant, showing it had the highest QoE of competing vendors at the lowest cost. Cisco and Microsoft do not offer nearly the same amount of functionality, ease of use, or intuitive interface as WatchGuard.

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. Additionally, every Firebox offers SD-WAN right out of the box for improved network resiliency and performance.



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. Empower the workforce with easy-to-adopt authentication tools, like single sign-on (SSO), to reduce password reuse and increase productivity. Leverage our dark web credential monitoring services to mitigate the risks of widespread credential attacks. AuthPoint also integrates with WatchGuard's ThreatSync Core, providing a unified view and the ability to respond to credential access incidents.



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

WatchGuard Endpoint Security solutions help you safeguard devices against cyber threats. WatchGuard EPDR and Advanced EPDR, our AI-powered flagship endpoint solutions, enhance your security posture by seamlessly integrating endpoint protection (EPP) with detection and response (EDR) capabilities alongside our Zero-Trust Application and Threat Hunting Services. All are tightly integrated within WatchGuard Cloud and ThreatSync, delivering valuable visibility and intelligence while fortifying cross-product detection and response (XDR).

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](https://www.watchguard.com).