Top Reasons to Buy WatchGuard Identity Security

AuthPoint identity security solutions include multi-factor authentication (MFA), advanced password generation capabilities, and secure password vaults. AuthPoint gives businesses the tools they need to stay secure in an increasingly digital world. Additionally, our dark web monitoring feature helps companies stay ahead of the curve by detecting compromised credentials before they can be used maliciously.

Key AuthPoint Identity Security Features and Benefits

Unlock advanced password generation capabilities and dark web monitoring to help protect corporate credentials

Award-Winning MFA Service

Delivered through WatchGuard Cloud, AuthPoint MFA makes it easy for users to authenticate with offline and online verification methods and access policies across endpoints, VPNs, and web applications. Efficient and secure access to Cloud resources is also available with single sign-on (SSO) application portals.
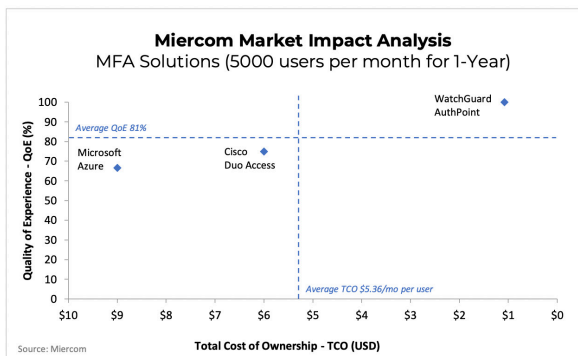
Dark Web Monitoring Service

AuthPoint's Dark Web Monitoring service proactively notifies customers when compromised credentials from up to three monitored domains are found in newly acquired credential breach databases. Alerts are sent to administrators and end users impacted so they can generate new passwords quickly and before account takeover.

Password Manager

Built with business use cases in mind, AuthPoint's Password Manager gives organizations a higher standard of strong passwords and can reduce password reset requests by generating passwords that do not need to be remembered. Additionally our password manager offers:

- **Corporate Vault** – Add credentials and generate strong passwords for commonly used workplace applications where you do not have SSO enabled. Plus, administrators can share credentials for the common use of IT applications and tools.

- **Private Vault** – Add credentials and generate strong passwords for personal and social app. If the employee leaves the organization, these personal credentials can be exported and used within another password manager.

Why Organizations Are Choosing AuthPoint MFA

Hybrid-Work Security Made Easy

Simplify password use with single sign-on (SSO) configurations that enable remote work with secure login and access to applications.

Seamless User Experience

Independent product validation shows AuthPoint as a top choice for first-time users thanks to its intuitive interface, helpful guides, and single-click setups – compared to other solutions on the market.

Mobile DNA for Secure Migration

WatchGuard's MFA solution includes a mobile device DNA functionality that automatically matches the authorized user's phone before granting access. Any attacker cloning a user's device to access protected systems is immediately blocked.

High Value and ROI

Compared to other solutions, WatchGuard delivers a rich set of native features, hundreds of integrations, and dedicated customer support, all for one fixed price per user per month.

Path to Zero Trust Adoption with Authentication Policies

AuthPoint's adaptive policies and controls enable unified access management, a key step for zero trust security adoption.

Miercom Market Impact Analysis
MFA Solutions (5000 users per month for 1-Year)

Source: Miercom

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.

WatchGuard Cloud

Key Identity Security Features

AuthPoint Mobile Authenticator App

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
SUPPORTED PLATFORMS
Android v7.0 or higher
iOS v12.5.7 or higher

AuthPoint Cloud Management

MANAGEMENT FEATURES
Administration, configuration and management with WatchGuard Cloud
Configurable authentication resources
Customizable authentication and risk policies (network, time, geofence and geokinetics)
Dark Web Scan of up to 3 domains
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

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 INTEGRATIONS **MFA with 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 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

Don't Take Our Word for It

TrustRadius ★★★★☆

"A reliable and cost-efficient 2 factor authentication for our customers. Mainly used for MFA VPN access for authenticated users to work remote. Before using WatchGuard AuthPoint, we did not have a good solution for all our customers in using MFA to connect to a VPN."

– Robbie Matthew, Senior Network Engineer
Invision Technologies, LLC (Telecommunications, 51-200 employees)