

AuthPoint Identity Security

AuthPoint Identity Security solutions include our award-winning multi-factor authentication (MFA), phishing-resistant passkeys, Windows and macOS logon protection, and single sign-on (SSO). Total Identity Security adds credential monitoring to help mitigate risks from workforce credential attacks.



MFA

Mobile authenticator app and hardware tokens (push, QR code, OTP)



FIDO2 Passkeys

Phishing-resistant authentication methods.



Cloud Management

Multi-tenant administration and reporting from WatchGuard Cloud



Zero Trust Policies

Risk-based access control with location, time, and travel conditions



Dark Web Monitoring

Credential breach monitoring across managed accounts

AUTHPOINT AUTHENTICATION METHODS	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
AUTHPOINT MOBILE AUTHENTICATOR APP		
AUTHENTICATOR TYPES		
Push Notification with Phishing Toggle (online mode)	●	●
QR Code Generator (online and offline modes)	●	●
Time-based One Time Passcode (online and offline modes)	●	●
Passwordless login with biometrics (Windows Hello, macOS Touch ID)	●	●
MFA prompt for privilege elevation (Windows UAC, macOS sudo) on protected endpoints	●	●
Offline authentication for the AuthPoint Logon App (Windows and macOS credential provider, QR code, and OTP)	●	●
SECURITY FEATURES		
MFA fatigue protection (Phishing Toggle and ThreatSync push abuse detection)	●	●
Jailbreak and Root Detection	●	●
Mobile Device DNA / SIM Swap Protection	●	●
Online token activation with Dynamic Key Generation	●	●
App Protection: PIN, fingerprint, and face recognition	●	●
Self-service, secure migration to another device	●	●
Multiple tokens per user and third-party token import	●	●
Token name and icon customization	●	●
SUPPORTED PLATFORMS		
Android 7.0 or higher	●	●
iOS 14.0 or higher	●	●
PASKEY AUTHENTICATION		
FIDO2 passkey authentication for OIDC and SAML resources	●	●
Phishing-resistant (cryptographically bound to origin domain)	●	●
Single passkey enrollment for both OIDC and SAML resources	●	●
Platform authenticator support (fingerprint, face scan, device PIN)	●	●
Roaming authenticator support (FIDO2 hardware security keys)	●	●
Passkey and MFA available together in the same policy (user chooses at login)	●	●
Self-service enrollment with email verification	●	●
Zero Trust policy integration per OIDC and SAML resource and user group	●	●

SUPPORTED PASSKEY RESOURCES		
WatchGuard FireCloud (Internet Access and Total Access)	●	●
Microsoft Entra ID via External MFA (formerly External Authentication Methods)	●	●
OIDC-connected applications	●	●
SAML-configured resources (AuthPoint as SAML Identity Provider)	●	●
SUPPORTED PASSKEY PLATFORMS		
Apple (iCloud Keychain)	●	●
Google (Google Password Manager)	●	●
Microsoft (Windows Hello)	●	●
FIDO2/CTAP2 hardware security keys (YubiKey 5 series, Bio series)	●	●
Credential managers that support Passkeys (like 1Password, Bitwarden)	●	●
AUTHPOINT CLOUD MANAGEMENT	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
MANAGEMENT FEATURES		
Multi-tenant architecture for Service Providers managing multiple customer accounts	●	●
Administration, configuration, and management with WatchGuard Cloud	●	●
Zero Trust policies with risk-based conditions (network, time, geofence, geokinetics)	●	●
Audit logs and reporting (up to 12-month retention)	●	●
Configurable authentication resources	●	●
Dark Web Credential Monitoring		●
Dashboard widgets for authentications, users, devices, and subscriptions	●	●
Easy deployment with integration guides and wizards	●	●
Synchronization with Active Directory and LDAP	●	●
Microsoft Entra ID synchronization via Directories and Domain Services (DDS)	●	●
WatchGuard Cloud Directory for users and groups management for customers without AD or Entra ID	●	●
RESTful Authentication API for custom application integration	●	●
ZERO TRUST POLICIES	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
POLICY COMPONENTS		
Policy assignment by user group and resources	●	●
Resource protection across OIDC, SAML, Firebox, RADIUS, Logon App, IdP Portal, RD Web, ADFS, and RESTful API Client	●	●
Allow and Deny policy actions	●	●
Multiple authentication methods per policy (Password, Push, QR Code, OTP, Passkey)	●	●
Priority-based policy precedence	●	●
ZERO TRUST CONDITIONS		
Network Location: authentication filtered by source IP or network	●	●
Time Schedule: authentication limited to specific days and hours	●	●
Geofence: authentication restricted to authorized countries	●	●
Geokinetics: impossible travel detection between consecutive logins (evaluated post-authentication)	●	●
DARK WEB CREDENTIAL MONITORING	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
CREDENTIAL MONITORING		
Monitors compromised credentials for all users of your managed accounts		●
Alerts in WatchGuard Cloud when user credentials appear in breach databases		●
Identifies which users are affected and the breach source across all managed accounts		●
Automated, continuous monitoring from a single console for all managed customers		●
Enables MSPs to deliver credential monitoring as a managed service		●

THREATSYNC INTEGRATION	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
CREDENTIAL ACCESS INCIDENT TYPES		
Login attempts with an incorrect password	●	●
Token blocked by too many failed authentications	●	●
User disabled push notifications	●	●
User received too many push notifications	●	●
Authentication denied by Zero Trust policy	●	●
Authentication attempt from an unknown user	●	●
REMEDATION ACTIONS		
Block a WatchGuard Cloud Directory user	●	●
Block an IP address in Firebox	●	●
Isolate an endpoint (requires WatchGuard Endpoint Security license)	●	●
AUTHPOINT COMPONENTS	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
AUTHPOINT GATEWAY & INFRASTRUCTURE		
Secure outbound connection from network to WatchGuard Cloud	●	●
RADIUS Server	●	●
Gateway runs on Windows Server 2012 R2 and higher	●	●
Up to 5 secondary Gateways per primary for LDAP authentication failover and backup RADIUS	●	●
High Availability multi-region deployment for Firebox authentication resources	●	●
AUTHPOINT AGENTS & SUPPORTED PLATFORMS		
macOS 10.11 (El Capitan) and above	●	●
Windows 10 or higher	●	●
Windows Hello for Business	●	●
Active Directory Federation Services on Windows Server 2012 R2 through 2022 (SSO)	●	●
Windows Server 2012 R2 and above logon	●	●
Windows Remote Desktop Web Access	●	●
Supported Browsers: Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari	●	●
HARDWARE TOKEN		
WatchGuard hardware token with no seed exposure	●	●
Support for third-party OATH TOTP tokens and multiple tokens per user	●	●
AUTHPOINT INTEGRATIONS	AuthPoint Multi-factor Authentication (MFA)	AuthPoint Total Identity Security
WATCHGUARD PLATFORM INTEGRATIONS		
FireCloud (Internet Access and Total Access) via SAML or OIDC with AuthPoint as Identity Provider	●	●
Firebox Mobile VPN authentication (IKEv2, SSL, L2TP, IPSec)	●	●
Firebox Authentication Portal	●	●
Firebox Web UI	●	●
Firebox Access Portal	●	●
WatchGuard Account SSO	●	●
WatchGuard Management Server	●	●
MFA WITH SINGLE SIGN-ON		
SAAS: Atlassian, BlueJeans, Box, Citrix, Confluence, Dropbox, Evernote, GitHub, Google Workspace, Go to Meeting, Jira, LucidChart, Microsoft 365, Salesforce, ServiceNow, Slack, Tableau, Webex and more...	●	●
IAAS: Adobe Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Oracle Cloud and more...	●	●
Security & Management: Akamai, BMC, Cisco, ConnectWise, CyberArk, Fortinet, ITGlue, JAMF, ManageEngine, Ivanti, PagerDuty, Delinea, VMware, WatchGuard Firebox, WatchGuard VPN, and more...	●	●

PRODUCT INFORMATION		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, and 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)		●	●
Argon2id Open Source (password hashing for credential storage in Dark Web Monitoring)			●
FIDO2/WebAuthn (W3C)		●	●
TRUST AND COMPLIANCE			
AuthPoint Authentication Service SLA : 99.99% uptime.			
WatchGuard Cloud is ISO/IEC 27001 :2022 certified.			

● *AuthPoint Total Identity Security Only Feature*