AuthPoint

MFA That's Powerfully Easy

Today's security landscape shows that using stolen credentials to breach network resources is the #1 tactic that hackers use. In fact, 80% of data breaches involve stolen or weak passwords as the main vulnerability.* Multi-factor authentication is the single most important security enhancement you need to protect your business.

WatchGuard's multi-factor authentication (MFA) solution not only protects identities, and reduces network disruptions and data breaches arising from weak or stolen credentials, but it delivers this important capability entirely from the Cloud for easy set-up and management. AuthPoint's unique mobile DNA technology goes beyond traditional 2-factor authentication (2FA) by incorporating innovative ways to identify and protect. With our large ecosystem of more than 130 third-party integrations, this means that strong protection can be consistently deployed across the network, VPNs, Cloud applications – wherever it's needed. Even non-technical users find the friendly AuthPoint mobile app easy and convenient to use. Ultimately, WatchGuard AuthPoint is the right solution at the right time to make MFA a reality for businesses who desperately need it to block attacks.

Risk Authentication for Zero-Trust Adoption

Zero-trust adoption cannot happen without identity protection, and with risk-based authentication being a core element of MFA, AuthPoint becomes a key solution to embrace the "never trust, always verify" approach. Without risk policies in place, your company would need to enable the most secure authentication method at all times, for all users, potentially causing user friction for some segments. With AuthPoint you have access to risk features at no additional cost, including Network Locations, Time Schedule, Geolocation functions and the exclusive mobile DNA, which prevents mobile token cloning.

A Low TCO Cloud-Based Service

Companies with limited IT staff and security expertise benefit from MFA protection that's easy to deploy and manage from the Cloud. AuthPoint runs on the WatchGuard Cloud platform and is available from wherever you are. There is no need to install software, schedule upgrades or manage patches. Moreover, the platform easily accommodates a single global account view or many independent accounts, so that distributed enterprises and managed service providers can display only the data relevant to a person's role.

Broad Coverage with Web SSO

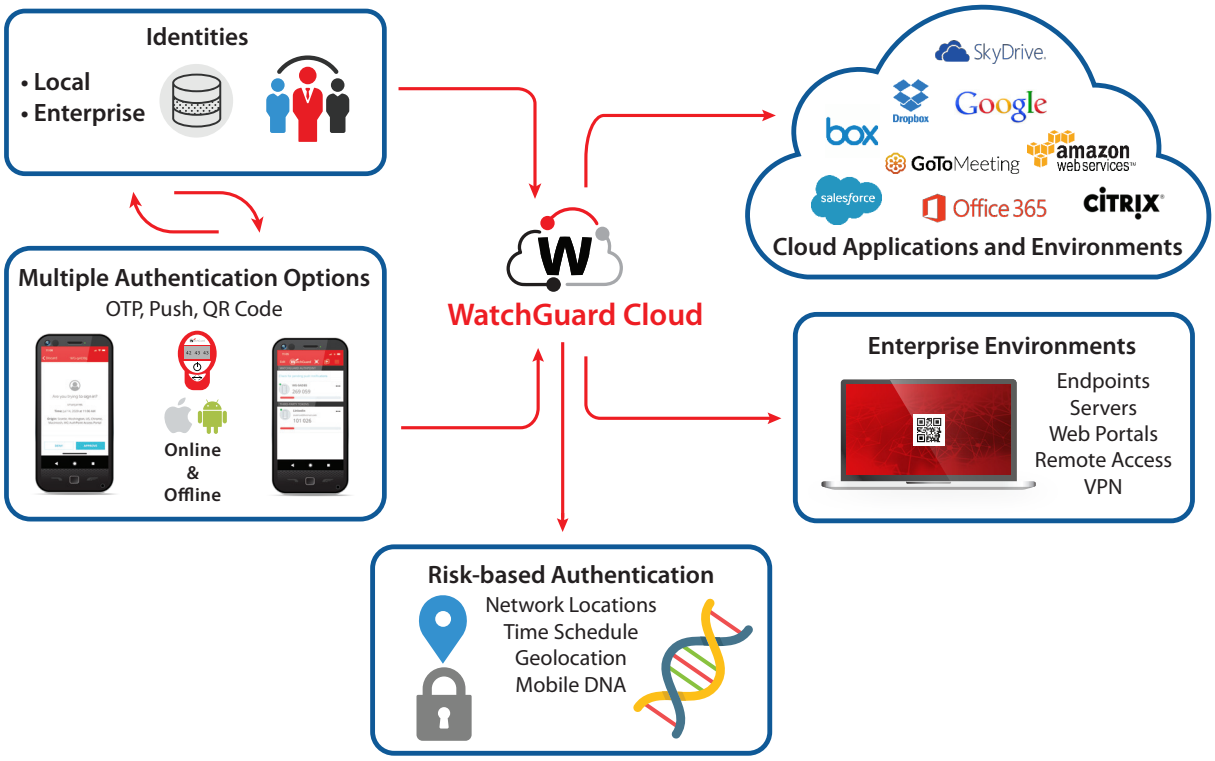
Stop worrying about remembering countless complex passwords. AuthPoint's secure single sign-on (SSO) makes it easier for users to access multiple Cloud applications, VPNs and networks with only one set of credentials. This combats the challenges presented by password fatigue and reduces risk of security vulnerabilities due to weak passwords and costs associated with password resets. AuthPoint supports the SAML standard protocol, permitting users to log in once to access a full range of applications and services. Our secure login feature also provides online and offline authentication to Windows and Mac machines using the AuthPoint app or hardware token.

User-Friendly Optimized Mobile App

Install and activate WatchGuard's AuthPoint app in seconds so you can authenticate from your smartphone. It not only enables speedy push-based authentication, but it also offers the pull authentication feature for better usability and security. It also includes offline authentication using QR codes with the phone's camera. The app is available in 13 languages and downloads free of charge from the App Store and Google Play.

**Verizon Data Breach Investigations Report 2020*

Keep Imposters Off Networks, VPNs, Cloud Resources and More!



WatchGuard Cloud Platform

- 100% Cloud-based management in three regions
- Powerful risk-based policy management
- Logs and reports
- Audit role-based access
- Intuitive, attractive user interface

AuthPoint Mobile App

- Three authentication options available:
  1. Push messages with guaranteed delivery
  2. One-time passwords (time-based)
  3. Challenge/response QR codes
- Mobile authenticator – no additional hardware to carry
- 13 languages
- Multi-token support
- iOS and Android – free to download
- PIN/biometrics protection
- Mobile device DNA – added authentication factor
- Self-service mobile token migration to new devices
- Third-party token support to protect personal accounts (Gmail. social media, etc.)

AuthPoint Gateway

- Corporate network gateway
- AD and LDAP user authentication and sync
- RADIUS proxy

AuthPoint Agents

- Integration with third-party applications without native MFA support
- Online, offline and RDP login protection for Windows and macOS
- Agent for RD web and ADFS

AuthPoint Ecosystem

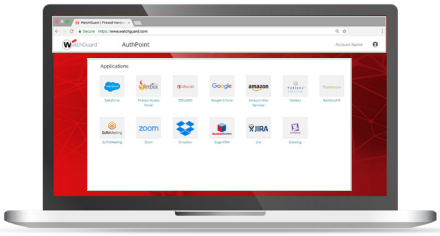
- Add MFA to Cloud resources, applications, databases and web resources
- Support for SAML and RADIUS standards
- More than 130 third-party integration guides including CRM and videoconferencing solutions
- Firebox direct integration with AuthPoint for fast VPN configuration
- AuthPoint Hardware Token with no token seed exposure and support for third-party hardware tokens (OATH TOTP)

Recommended Use Cases

VPNs / Remote Access

Same user experience as username + password BUT more secure, and with a single-click confirmation. Integrates with any firewall, but especially with out-of-the-box Firebox appliances.

1. Request connection with username & password
2. Confirm VPN connection – request through AuthPoint app



Cloud Applications – Web SSO

1. Access the Identity Portal (IdP)
2. Authenticate using OTP, push or QR code
3. Access all the apps assigned to you with only one password. No need to authenticate again!

PC Login or RDP Connection

1. Log in to Windows/Mac with username + password
2. Choose preferred authentication method (Push, QR code or OTP)
3. Approve on your phone. Login is done!

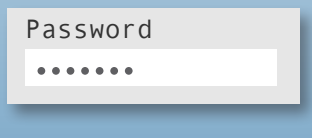
PC Login – Offline Authentication

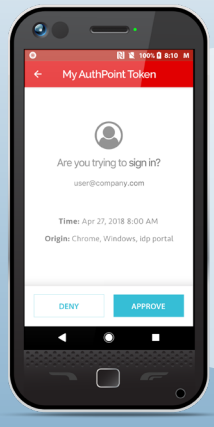
1. Log in to Windows/Mac with username + password
2. Scan the QR code (or OTP) using the AuthPoint App
3. In this example, you would type the response 717960

What Is Multi-Factor Authentication (MFA)?

Use of 2 or more authentication factors, from:

- **Something you know** (password, PIN)
- **Something you have** (token, mobile phone)
- **Something you are** (fingerprint, face)





AuthPoint factors:

1. **Your password**
2. **Approval on your mobile authenticator**
3. **Correct mobile phone DNA**
4. **A fingerprint to access** (with certain phone models)

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

Making the Case for MFA

Weak passwords are a serious liability for your business. **The average user has almost 100 online accounts**, many of which have their own password requirements. Password fatigue is a real problem and it's putting your business at risk. It takes just one weak or cracked password for a cyber criminal to access all your data and accounts.

How confident are you that every single employee is following password best practices?

- Roughly 250,000 passwords are stolen every day[1]
- Only 1 in 5 users uses a unique password across all accounts[2]
- 3% of people use the password 123456[3]

> "Through 2021, enterprises that rapidly expand remote access without implementing MFA will experience five times as many account takeover incidents as those that use MFA."
>
> Gartner, Inc., Enhance Remote Access Security With Multifactor Authenticationand Access Management
> Ant Allan, Rob Smith, Michael Kelley, May 6, 2020

The cost of a breach can be enough to put your company out of business. **The average cost of a data breach is $148 per data record** with sensitive information, which is $1.38 million when you consider the average data breach of 9.350 records. This doesn't include indirect costs like a damaged company reputation, lost customer trust, and lost work time.

The good news is that you can easily reduce your cyber risk and get a high return on your security spend. It costs less than the price of your morning Starbucks to provide monthly MFA protection for each employee. Eliminate the #1 risk to your business with AuthPoint.

Want to try it out? Visit **watchguard.com/TryAuthPoint** or contact one of our dedicated specialists to get started with a free 30-day trial.

1 https://breachalarm.com/
2 https://www.statista.com/statistics/763091/us-use-of-same-online- passwords/
3 https://www.techspot.com/news/77864-worst-passwords-2018-revealed-123456-retains- top-spot.html

THE WATCHGUARD UNIFIED SECURITY PLATFORM™

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Secure Cloud Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyber attacks. Its flagship solution, WatchGuard EDPR, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit **www.watchguard.com**.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.