



# AuthPoint

## MFA That's Powerfully Easy

Using stolen credentials to breach network resources is the #1 tactic that hackers use.\* By requiring additional proof of identity beyond a simple password, multi-factor authentication is the single most important safeguard to protect your business.

WatchGuard's unique multi-factor authentication (MFA) solution not only reduces network disruptions and data breaches arising from weak or stolen credentials, but we deliver this important capability entirely from the Cloud for easy set-up and management. Moreover, AuthPoint® goes beyond traditional 2-factor authentication (2FA) by incorporating innovative ways to identify users, such as with our Mobile Device DNA. With our large ecosystem of 3rd 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.

### Effective MFA Protection with Mobile Device DNA

Multi-factor authentication requires users to supply information they know (username and password), and information provided on something they have, as well as other factors that can be associated to the specific individual. AuthPoint provides a highly secure MFA product using a push message, QR code, or one-time password (OTP); and our mobile device DNA matches the authorized user's phone when granting access to systems and applications. Therefore, any attacker who clones a user's device in an attempt to access a protected system would be blocked, since the device DNA would differ.

### Easy-to-Use AuthPoint Mobile App

WatchGuard's AuthPoint app allows users to authenticate right from their own phone! No need to carry key fobs or thumb drives; instead install and activate the AuthPoint app in seconds, and then use it to authenticate from a smartphone. It enables speedy push-based authentication as well as 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.

### Broad Coverage with Web SSO

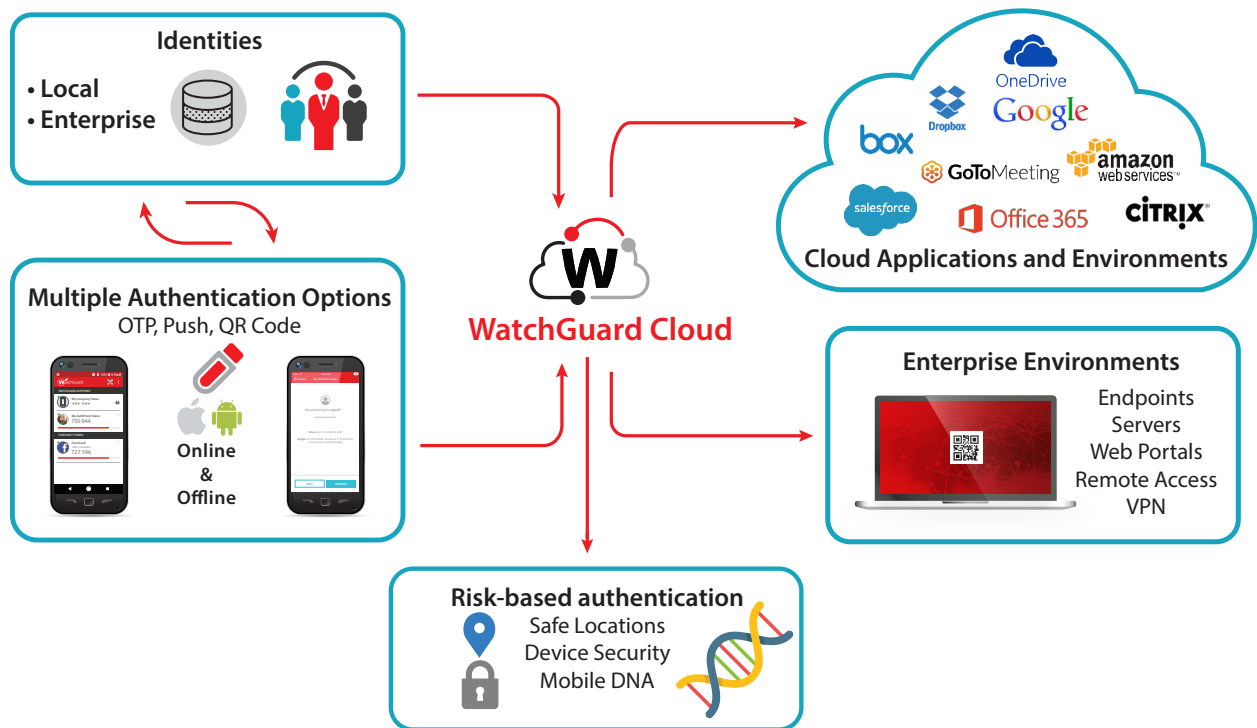
Stop worrying about remembering countless complex passwords. AuthPoint's secure single sign-on (SSO) makes logins quick and easy. In addition WatchGuard's ecosystem includes dozens of 3rd party integrations with AuthPoint – allowing companies to require users to authenticate before accessing sensitive Cloud applications, VPNs and networks. AuthPoint supports the SAML standard, permitting users to log in once to access a full range of applications and services. In addition, the secure login feature provides online and offline authentication to Windows and Mac machines using the AuthPoint app.

### 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.

\*Verizon Data Breach Investigations Report 2018

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



### WatchGuard Cloud Platform

- 100% Cloud-based management
- Authenticator allocation and activation
- Authentication policies based on groups and resources
- Logs and reports
- Role-based access
- Intuitive, attractive user interface

### AuthPoint Mobile App

- Three authentication options available:
  1. Push messages
  2. One-time passwords (time-based)
  3. QR codes when offline
- Mobile authenticator – no additional hardware to carry
- 13 languages
- Multi-token support
- iOS and Android – free to download
- PIN/biometrics protection (on certain devices)
- Mobile device DNA – added authentication factor
- Self-service mobile token migration to new devices

### AuthPoint Gateway

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

### AuthPoint Agents

- Integration with 3rd party applications without native MFA support
- Computer login protection for Windows and macOS

### AuthPoint Ecosystem

- Add MFA to Cloud resources, applications, databases and web resources
- Support for SAML and RADIUS standards
- Comprehensive integration guides for many popular 3rd party solutions

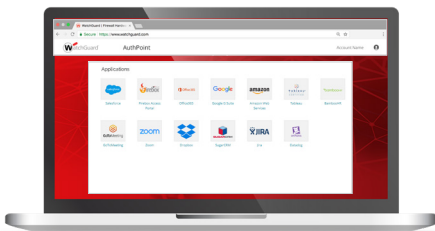


## Recommended Use Cases

### VPNs / Remote Access

Same user experience as username + password BUT more secure, and with a single-click confirmation.

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 to which you are entitled – no need to authenticate again!

### PC Login – Online Authentication

1. Click on “Send push”
2. Confirm PC login request through AuthPoint app
3. Login is done



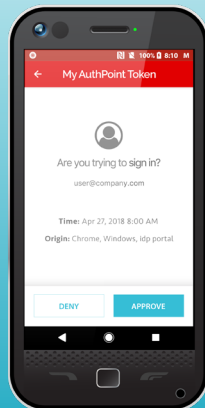
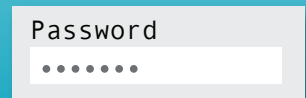
### PC Login – Offline Authentication

1. Select “QR code” to authenticate
2. Scan the QR code 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<sup>1</sup>
- Only 1 in 5 users uses a unique password across all accounts<sup>2</sup>
- 3% of people use the password 123456<sup>3</sup>

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](https://watchguard.com/TryAuthPoint) or contact one of our dedicated specialists to get started with a free 30-day trial.

<sup>1</sup> <https://breachalarm.com/>

<sup>2</sup> <https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/>

<sup>3</sup> <https://www.techspot.com/news/77864-worst-passwords-2018-revealed-123456-retains-top-spot.html>

## THE WATCHGUARD SECURITY PORTFOLIO



### Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing managing, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.



### Secure 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.



### Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

## Find out more

For additional details, talk to your authorized WatchGuard reseller or visit <https://www.watchguard.com>.

## About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. WatchGuard 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).