aws marketplace

WatchGuard AuthPoint MFA

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

WatchGuard AuthPoint MFA

WatchGuard AuthPoint MFA Recap

WatchGuard AuthPoint MFA enhances security with push authentication for Android and iOS without hardware tokens. It offers a user-friendly experience via mobile notifications and approvals, bolstering workforce authentication effectively.

WatchGuard AuthPoint MFA provides robust security through easy-to-use multi-factor authentication, compatible with Android and iOS. Its push authentication eliminates the need for hardware tokens, streamlining user experience with convenient mobile device notifications. The integration with platforms like AWS and Office 365 secures remote work and prevents credential theft. With WatchGuard firewall features like UDP and GeoBlock, roles are easily established for advanced connection control. Enhancements like improved documentation and video tutorials could further support users. The solution's alignment with GDPR, zero trust features, and expanded laptop management make it versatile for security needs.

What are the key features?

- Push Authentication: Offers seamless Android and iOS compatibility without hardware tokens.
- Mobile Management: Provides notifications and approvals managed via mobile devices.
- Secure Integrations: Easily integrates with platforms like AWS and Office 365.
- Firewall Security: Utilizes advanced features like UDP, block filters, and GeoBlock.
- Role Establishment: Allows connection control through established roles.

What benefits should users expect?

- Enhanced Security: Multi-factor authentication effectively prevents unauthorized access.
- Improved Experience: Mobile notifications and integrations increase usability.
- Adaptability: Suitable for sectors like banking to secure sensitive data effectively.
- Easy Implementation: Straightforward syncing with local gateways and directories.

In sectors such as banking, WatchGuard AuthPoint MFA is crucial for securing VPN access and protecting sensitive data. It integrates seamlessly with existing WatchGuard VPNs to bolster security measures. Its easy implementation makes it an attractive option for securing remote work and preventing credential theft, offering particular value for banking institutions looking to enhance data protection strategies.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The WatchGuard firewall includes many security features, such as UDP, block filters, web filtering, and GeoBlock."

Verified user
IT Manager at a financial services firm with 1,001-5,000 employees

- "The token-based two-factor verification (2FA) for user logins is valuable. It's the primary reason we use AuthPoint, and I find it very effective."

Michael-Angelo Francis
Senior IT Tech at PCSL

- "The initial setup is very simple."

RuiBarbosa
IT Director at Wingsys

- "The integrations are good."

Ícaro Lira
Network Administrator at SuporteOne

- "The approvals feature of this solution is very good; it is operated by just one button, and can be controlled from a mobile device if needed."

Mohamed Y Ahmed

Technical & Pre-Sales Manager at GateLock

- "Personal notifications are very easy to use."

Verified user

IT Technician at a real estate/law firm with 11-50 employees

- "It can be implemented as an app on the phone, rather than with a hardware token."

RainerAlbrecht

General Manager at Gemakom

What users had to say about valuable features:

"The WatchGuard firewall includes many security features, such as UDP, block filters, web filtering, and GeoBlock. It's advantageous for us to have the roles in place to block people where we want to have them connected.."

Verified user
IT Manager at a financial services firm with 1,001-5,000 employees

Read full review

"The solution helps with workforce authentication. The security provided by the product is valuable. It is easy to use the push notifications. They improve user experience. The integrations are good.."

Ícaro Lira
Network Administrator at SuporteOne

Read full review

"Push authentication is very, very compatible and a valuable feature. You only need a smart phone, Android, or iOS and then it can be implemented as an app on the phone, rather than with a hardware token. There's no need to wear a hardware token so you're always secure. Your smart phone is by your side and so is your token. If it were a hardware token you would have a big problem.."

RainerAlbrecht
General Manager at Gemakom

Read full review

ROI

Real user quotes about their ROI:

“We saw a very high ROI. Since we started reselling and using WatchGuard as our flagship, it's evolved beyond firewalls to a SaaS platform offering comprehensive cybersecurity.

This allows us to sell its value and market the products to customers, earning profit through our markups. Additionally, WatchGuard's excellent support and service quality contribute to our company's overall return on investment. We trust them and they are reliable..”

Michael-Angelo Francis
Senior IT Tech at PCSL

Read full review

Use Case

"We mainly use this solution to provide security for the devices on our clients network in the banking sector; to stop credential theft, or virus transfer from staff working remotely.."

Mohamed Y Ahmed
Technical & Pre-Sales Manager at GateLock

Read full review

"WatchGuard AuthPoint is the multifactor authentication solution for our VPN. It gets used on a regular basis. It is our multifactor authentication piece to connect to our VPN back into our network.

We are using its latest version. It is a cloud solution, and it is probably onWatchGuard's cloud. We don't control it.."

Verified user
IT Technician at a real estate/law firm with 11-50 employees

Read full review

"We use the product for multi-factor authentication in-house. We also expect our suppliers to implement the solution because we're dealing with sensitive data, personal data, and need to use two-factor authentication. So it can be integrated with remote support. We use well-prepared templates to integrate the AWS, Office 365, and so it's very, very easy to implement for our needs. I'm the General Manager of our company and we partner with WatchGuard.."

RainerAlbrecht
General Manager at Gemakom

Read full review

"We had a client needing strong security measures for their VPN users. They already used WatchGuard VPN, so to add extra security, we recommended upgrading their basic subscription to include multi-factor authentication (MFA) with AuthPoint. It was seamless, applying the license, adding users, syncing with the local gateway, then Active Directory, and the user groups. And it was as easy as that.

I primarily use AuthPoint for the authentication feature, and it can also do mobile device authentication and more.."

Michael-Angelo Francis
Senior IT Tech at PCSL

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"It is fairly straightforward. You need to have some general knowledge of networking and networking functions, but other than that, it is pretty straightforward.."

Verified user

Read full review

IT Technician at a real estate/law firm with 11-50 employees

"Initial setup is quite straightforward. The customer just needs to instal the gateway software on premise. It's a RADIUS emulation. Deployment takes about half an hour. The time it takes depends on the number of users that you want to implement. Every user needs a token and implementation is on the smart phone so it can take more time, but for one end user deployment takes half an hour.."

RainerAlbrecht

Read full review

General Manager at Gemakom

“The initial setup with AuthPoint was very easy. I simply logged into WatchGuard Cloud, entered the license, and attached it to the necessary firewall. The wizards were clear and straightforward, with no guesswork involved.

Once I configured the gateway and put it on a server, the configuration for specific features, like the Redis server, was clearly outlined. Everything went seamlessly.

It only took me around three hours! I needed a couple of support calls for questions that weren't explicitly covered in the instructions for advanced features, but the overall process was smooth and quick..”

Michael-Angelo Francis
Senior IT Tech at PCSL

Read full review

Customer Service and Support

“We've used technical support very rarely – reaction time is somewhere between two to four hours by email. You need a good reseller or system integrator because WatchGuard support is in English. We are in Germany so it's a bit of a disadvantage for native German speakers. But in the IT field it's normal to have to speak English. .”

RainerAlbrecht
General Manager at Gemakom

Read full review

“I have a couple of open cases right now as I explore the full potential of WatchGuard solutions and how they can help us.

Their accuracy has been impeccable, and their speed is fantastic. They're very responsive and technically competent. When I faced an issue configuring my CMITsec (local machines not pulling licenses from the IPSec server), it was a simple fix. The support technician walked me through the steps, and identified a missing firewall rule on port 22, and it was resolved within 15 minutes. Case open, case closed! The issue was fixed quickly. .”

Michael-Angelo Francis
Senior IT Tech at PCSL

Read full review

"Technical support needs more people who have good technical skills and knowledge instead of just sharing documentation. We can refer to the documentation from our end. It will be easy for us to troubleshoot if they have someone with knowledge of how these boxes work. We contact technical support when we can't find the issue after referring to the documentation. So, when they offer us documentation, it makes no sense.

We need someone with that knowledge level to understand the issue and at least recommend what needs to be done. Documentation sharing is something I can agree with. However, they share the document for any issue and ask us to refer to it. Having a TAC in place doesn't make sense if they don't want to resolve something in real time.."

Verified user

IT Manager at a financial services firm with 1,001-5,000 employees

Read full review

Other Advice

“Test the solution before you buy. There is a 30-day free trial period with full functionality, and it's easy to test. It's very, very important to use a multifactor authentication, and AuthPoint offers two-factor authentication with the various options.I would rate the product an eight out of 10. .”

RainerAlbrecht
General Manager at Gemakom

Read full review

“We would recommend that businesses considering this solution make sure that they know the business needs that apply to this product, in detail. They should also ensure that they have set up the policies before activating the hardware tokens, and before activating the MFA's that will be in place.

I would rate this solution a nine out of ten..”

Mohamed Y Ahmed
Technical & Pre-Sales Manager at GateLock

Read full review

“I'd suggest to read the documentation carefully. Reading the manuals is crucial. WatchGuard is detailed and clear, even for non-technical users. Its support team is also fantastic if you need further assistance.

The manuals cover everything from basic setup to advanced features like Intrudy WebUI and console monitoring. It's truly simple and straightforward.

Overall, I would rate the solution a nine out of ten..”

Michael-Angelo Francis
Senior IT Tech at PCSL

Read full review

“WatchGuard AuthPoint works well in securing remote access for our organization. It's helping the organization a lot in terms of people. Regarding remote connectivity, we have configured the solution with all the users using it.

The AuthPoint mobile app is used for AuthPoint authentication and push notifications. It's quite good in terms of performance, and I didn't find many issues with that. You get notifications on time, and it's working well.

The solution's push notification feature has provided a good user experience. I didn't find many delays in the notification process. It is quite reliable, and the notifications are coming on time to the users who didn't find any issues.

The product has limited next-generation firewall features. The solution has basic features but must improve and add many features to benefit the organization. That's something they need to develop.

I would recommend WatchGuard AuthPoint to people who have budget constraints and need a pretty standard solution with all the features that will benefit an organization. However, the solution has some limitations. People who want a higher level of packet capturing and something better in terms of deep-level

inspection should choose some other tool.

Overall, I rate the solution an eight out of ten..”

Verified user
IT Manager at a financial services firm with 1,001-5,000 employees

Read full review

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944