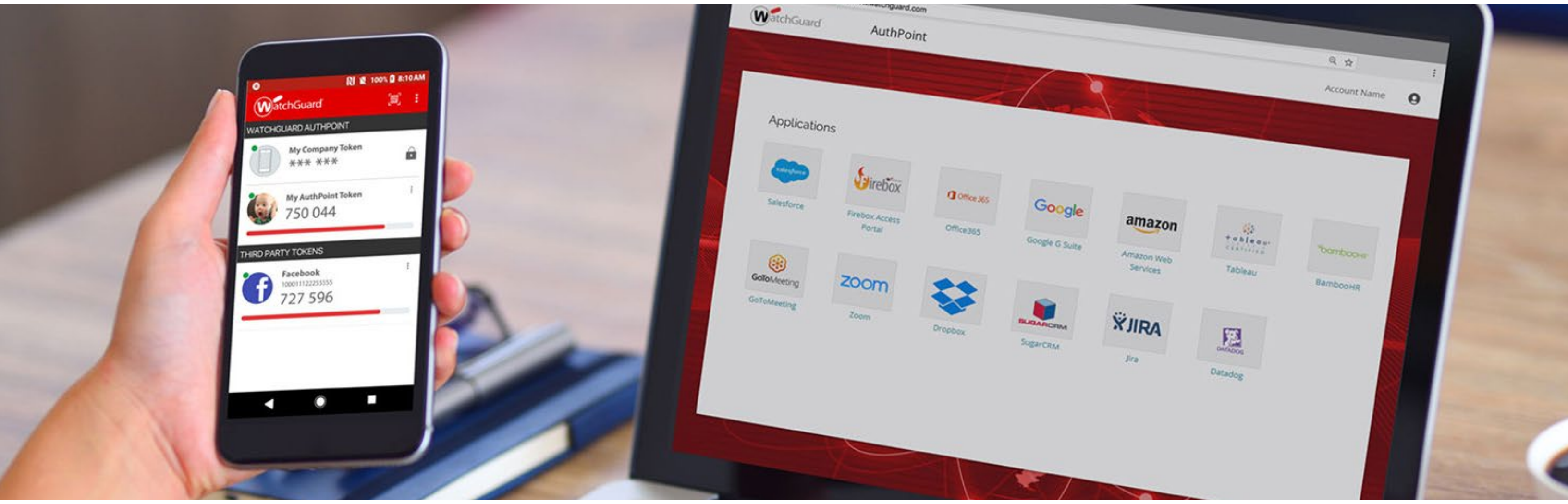
WHITEPAPER

Protecting User Identity and Securing Business Trust with Multi-Factor Authentication

Table of Contents



THE EVOLUTION OF AUTHENTICATION – HOW WE GOT HERE AND WHERE WE ARE NOW

The Authentication Problem

The Internet changed the way we do business. The access to fast Internet at home, as well as through millions of Wi-Fi hotspots in public places, allows employees to work from anywhere – their homes, hotels, coffee shops. Corporate information is not concentrated anymore in server rooms or data centers on premises; it is distributed in the Cloud, through CRM, email servers, web portals.

Every single day, an employee will certainly authenticate to several of those services. First, to their computer. Then, to an email server, and maybe a Cloud application. If they are not physically in the office, they are probably connecting to the network through a VPN. And where are the user credentials? The data traffic carries user credentials through Wi-Fi connections and public networks.

If at some point any of those credentials are exposed, what are the odds that the same password is used on most of the other services? The chances are high. With dozens of credentials to remember every day – corporate, banks, credit cards, eCommerce sites, social media, mobile stores, etc. – who would intentionally select a different password for each one of those services?

A password that is captured when you access your favorite grocery store website is likely to be the same password that you use to log in to your computer, or even worse, to the VPN that connects you to the corporate network. As we can see, the password problem goes beyond our corporate network. We cannot predict if an employee will use the same password for any type of personal service they have, or even if they at some point shared the password with someone.

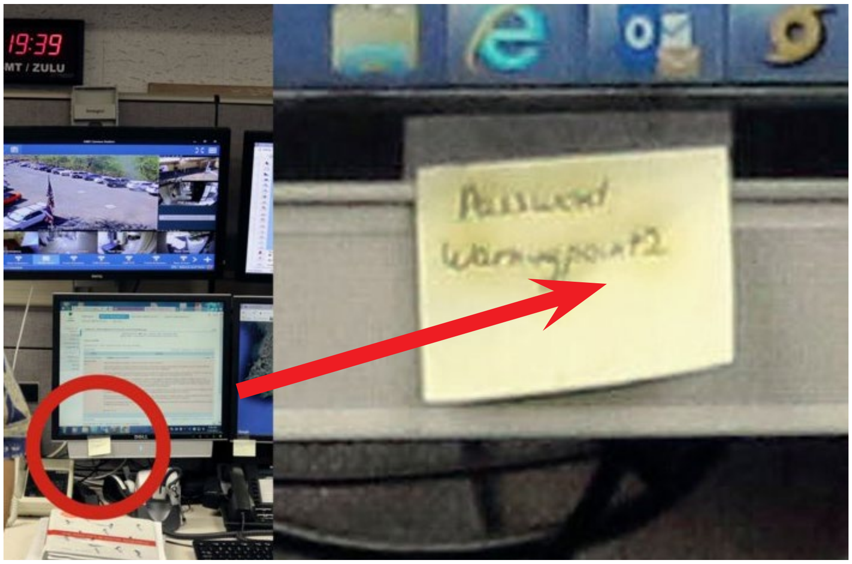
All of that is to say that we can't trust passwords. They can be shared. Written down. Captured. Guessed. Cracked. Stolen.

OVER
80%
OF BREACHES WITHIN HACKING INVOLVE THE USE OF LOST OR STOLEN CREDENTIALS.

Verizon Data Breach Investigations Report, 2020

Stolen Credentials and the Dark Web

The dark web is a collection of anonymous websites that are publicly available yet hide the IP addresses to make it impossible for users to identify the host. It's very common that sensitive information made available by data breaches ends up becoming available illicitly for sale on the dark web.
According to the 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses report, 63% of businesses reported an incident involving the loss of sensitive information about customers and employees in the past year.



Take for example, the recent database of Zoom credentials, exposed on the dark web in April 2020. However, there is no sign that Zoom was breached. In fact, the database was built up with credentials found in the dark web, that were tested against Zoom. And more than 500,000 credentials worked against Zoom accounts.

While your company might not have been hacked, employees might have their credentials available in the dark web after a breach within a service they use, like LinkedIn or Facebook. And since users tend to use the same passwords for multiple services, there is a great chance a corporate password could be the same as the one exposed by a different service breach.

Multi-Factor Authentication

The term "two-factor authentication" or "strong authentication" is not new. It started being used in the 90s, usually designating a hardware token generating one-time passwords (OTPs) associated with a fixed password. In fact, two-factor authentication refers to when you use two of the following factors:

- Something you know: a password, a PIN
- Something you have: a token, a physical device, a key
- Something you are: your fingerprint, face recognition

The technology evolution, especially with smartphone usage and app development growth, opened the possibility of putting together more factors, without compromising usability. When two or more factors are used, we now called it multi-factor authentication (MFA). WatchGuard AuthPoint is a good example of MFA being applied using four factors for an authentication.

The use of multiple factors will enhance the overall security of the solution, offering additional protection against several types of attacks such as social engineering and RATs (remote access trojans) designed to clone applications.

WHY MULTI-FACTOR AUTHENTICATION (MFA)?

These are standard authentication factors that MFA solutions could use:

1. Something you know

(your password)

2. Something you have

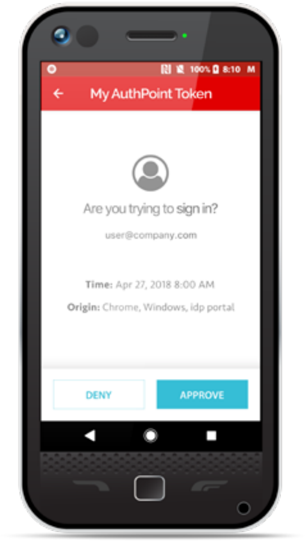
(a token on your phone)

3. Something you have

(a phone DNA)

4. Something you are

(a fingerprint to access)



Are you trying to sign in?

user@company.com

Time: Apr 27, 2018 8:00 AM

Origin: Chrome, Windows, idp portal

Security vs. User Experience

The first authenticators – or one-time password tokens, as they were called – were usually delivered as a hardware device, in a form and size usually a bit larger than a key fob. The OTPs were usually changing every 60 seconds, and to authenticate to a system, the user would need to type in the password followed by the OTP shown in the display. So, let's say their password was "mypassword", and the token was currently showing "122134". The user would need to enter:

```
myusername
mypassword122134
```

Not to mention the fact that the user would need to carry the key fob everywhere. The fact it was a physical key fob would only make things worse. If you have used a key fob token in the past, there is a very good chance that at some point you either forgot it at home and you had to ask someone to give you the OTP over the phone – repeatedly, or you went on a trip and left the token attached to your car keys, which were at home.

Often, security professionals said that usability is inversely proportional to security. This was a fact, and it would get worse. Users with connected tokens or smartcards and their readers would need to install software, middleware, and manage digital certificates – with a huge Total Cost of Ownership (TCO). And if they had to use those to authenticate into mobile applications, good luck connecting them!

By the end of the 2000s decade, mobile phones were improving, but there were still different operating systems and vendors. Symbian, BlackBerry OS, Windows Mobile, BREW, the list goes on. Developing an app for a phone was a hard task. You needed the vendor's SDKs and had to have a collection of various phone models. Running a Java app involved installing J2ME software, and the visual results were not appealing until the smartphone market started to grow, pushed and polarized by Android and iOS. This enabled companies to develop professional apps, following usability guidelines, with the same format for menus, buttons, etc. That's when mobile tokens started becoming popular.

The smartphone became part of our lives, like wearing clothes. If you are carrying your smartphone around, why do you need to carry hardware tokens?

And push technology finally changed the paradigm of usability vs. security. It resulted in better security, with improved user experience.

Push Technology

BlackBerry presented "push" as a technology that could indeed enhance productivity. The major advantage of having a BlackBerry was that you could see, almost instantaneously, when a new email arrived at your phone. The red blinking light of the BlackBerry became part of our lives.

The evolution of iPhones and Android devices drove push services to be used for different applications. Chat, news, emails. You didn't have to open your phone and connect to a service anymore, notifications were coming through that new channel.

And that opened up new possibilities for MFA. Instead of opening the mobile token app, reading the OTP and typing it in, you could now receive the authentication request on your phone, with more detailed information, such as who is trying to authenticate, and where. And all you needed to do was approve it by simply pushing a button, or reject it. It connected back to the service requesting the access and, if correctly implemented, the unique OTP was securely sent back without the user even knowing what it was.

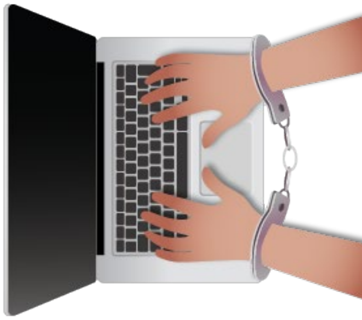
Now there is something that can provide better usability with a push-of-a-button user experience, so you know where you are authenticating to, and securely – through MFA.

WHERE WE ARE NOW

The COVID pandemic moved millions of employees to their homes and then the Internet became their daily commute. The working hours are also somehow gone. Working from home means the – home – office is always available.

What are some of the increased risks when large numbers of people are living their lives remotely? Let's be real, work-from-home employees are more exposed without having the security of firewalls and company Wi-Fi networks, and unfortunately, hackers are already jumping at the opportunity to attack vulnerable users. With the unprecedented events we are experiencing, it is fundamental to think about protecting remote employees to make sure company assets and information are accessed securely to prevent data and economic losses.

The working from home movement is here to stay once the pandemic is over and companies are evaluating the possibility of maintaining remote work or a hybrid model. In terms of cybersecurity, that means the idea of a more centralized and well-defined network is simply not enough anymore.
This brought with full strength the concept of the zero-trust approach. The network is now made up of applications, services, and groups of users and devices that needs access to them. Users and devices are everywhere, thus cannot be trusted. The use of MFA became a requirement to establish trust, especially now in this new hybrid work model.



WHY ALL BUSINESSES NEED MFA

The Remote Work Era

As companies grapple with having the predominance of their workforce working remotely, securing access to internal tools presents a major challenge. At the same time, hackers are increasingly targeting credentials, placing your users' account information directly in their crosshairs. Enabling MFA will protect the remote access to the network and Cloud applications against identity theft, using your own phone as another authentication factor.

Four main areas where MFA protects companies and remote employees:

- VPNs/Remote Access: Protects remote users with RADIUS protocols
- Cloud Applications: Eliminates the risk of weak passwords causing a data breach
- Computer Logons: Protects your employee logins and prevents unauthorized users from accessing your computer
- Web portals and home-developed applications

VPNs / Remote Access

Remote access to the company's network is key for remote and traveling users to access company servers and internal information. But all it takes is:

- one user with a bad password that was cracked
- one user with a keylogger trojan in the computer
- one user sharing their password or even OTP

And the hacker, anywhere in the world, now has access to the network, most of the time with the same privileges as someone physically sitting inside the company's premises, connected to the network.

What's needed is for an additional identity check, beyond password, before allowing users to access VPNs. Furthermore, the MFA solution should provide fast and easy integration with firewalls and remote access gateways using the RADIUS protocol. For example, with WatchGuard's AuthPoint MFA service, the set-up can be done in a few minutes and accomplished in two-ways:

1. **Using Password + OTP**

   Different than just typing in the username and password on a VPN client or browser-based clientless VPN, the user would just need to append the OTP – usually 6 digits – to the end of the password. The firewall will receive the request, and forward to AuthPoint, which will validate both password and OTP.

2. **Using Password + Push**

   This method provides the best user experience, since it doesn't much change the way it is used now. The user will still type in their username and password, as before. The difference is that AuthPoint will send an authentication request using push. The user will receive that message on their app, telling exactly who and where someone is trying to authenticate to. If the user is the person identified, all they need to do is approve with a single click of a button.

Authentication Method	Pros	Cons
Legacy OTP	• Typical, well-known method, in use for more than 20 years.	• Subject to social engineering • User needs to type in the OTP every time • Could be confusing for some users (password + OTP or OTP + password?)
Push	• Better user experience; user just needs to approve or reject • Better visibility; push message shows the context of the authentication, and reduces chance of social engineering • Better security; OTP sent within push cannot be copied or stolen	• Requires a data connection from the mobile phone (online authentication)

Cloud Applications

With the growth of Cloud applications and offerings, trivial but essential services started to move to the Cloud, such as email and web servers. Installing and maintaining those servers inside the network is now unthinkable. Cloud services offer almost anything you can think of, including CRMs, ERPs, development platforms, etc.

With all of those services, new challenges are surfacing:

- How users will be able to remember and maintain different passwords to the services
- Users must bookmark URLs and try to organize all services they potentially have access to
- How to make sure that a compromised credential won't give access to other services, which are easily accessed from anywhere in the world

SAML (Security Assertion Markup Language) protocol was created to solve most of these issues. Its implementation is based on two main entities:

- Identity Provider (IdP): an entity that will be responsible to properly authenticate and identify users
- Service Provider (SP): any entity that has a trust relationship with an IdP, and uses it to verify the identity

As a very simple way of looking into it, an SP will have a trust relationship with the IdP, meaning that, if the IdP authenticates and identifies a user, the SP will rely on that information to single sign-on the user into the service – even if the user has a different password for the service. Examples of SPs are Firebox® Access Portal, Salesforce, Google Apps, BambooHR, Jira, Office365, and others.

With that in mind, it is quite easy to understand that the IdP holds the key to the castle. Once the IdP authenticates the user, they will have Single Sign-On (SSO) access to all Cloud applications that were made available to this particular user. Therefore, choosing the right IdP is critical.

Cloud-based MFA solutions have the opportunity to provide an IdP service. For example, within our AuthPoint solution, a subscriber will have an exclusive portal to authenticate users. Once authenticated, the user will have access to the Cloud applications associated with their group. This provides enormous benefits in terms of security and user experience.

- User just needs to bookmark the IdP portal page
- The main authentication method can be configured to ensure higher security – for example, push-based authentication instead of legacy OTP
- User doesn't need to remember all Cloud application passwords. Once AuthPoint IdP portal authenticates the user, a trust relationship is established with the Cloud applications
- Group policies allow administrators to define exactly which applications each user is entitled to access
- If a credential was compromised, MFA will still take place, but block access by unauthenticated cyber criminals

Laptops / Computers Logon

Again, user credentials can be stolen, cracked, guessed. An unattended computer can potentially be accessed by someone in possession of those credentials. This can happen on company premises, and can happen with remote or traveling employees.
The use of MFA for computer login not only protects the login process but can also provide a better user experience.

AuthPoint Logon App is a component that can be installed on Windows and macOS computers, adding MFA capabilities within the login process. After entering the username and password, the user will receive a push message within the AuthPoint app, questioning if you approve login into your computer. The user experience is even improved when the user locks the computer. In this case, there is no need to reenter the username and password. All you need to do is approve the login by receiving the push message.

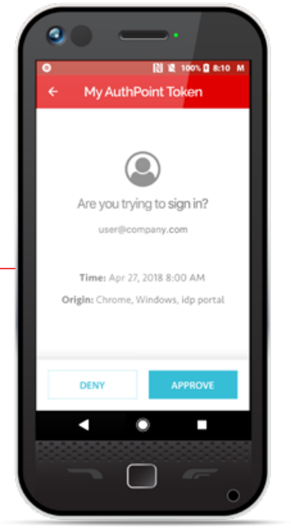
The versatility of the solution also provides a method of login into the computer when no Internet is available – the offline mode. This is important for situations such as using the laptop during a flight. In those cases, a challenge/response can be use, through a QR code with encrypted data that only the user's AuthPoint authenticator will be able to read, decrypt, and generate the response.

STEP 1

Click on "Send push"

STEP 2

Confirm PC Login request through AuthPoint app


My AuthPoint Token

Are you trying to sign in?

user@company.com

Time: Apr 27, 2018 8:00 AM

Origin: Chrome, Windows, idp portal

DENY APPROVE

STEP 3

Login is done!

Web Portals

Some companies provide services and solutions through web portals and offer user accounts to provide better user experience, especially for businesses in industries like education, healthcare, and retail, just to name a few. Having a user accounts can improve the way people interact with different information like health data, eLearning or any other service that might require a secure method of identification, especially with the growth of privacy laws enforcement around the world.

Modern business applications will implement standards to support MFA authentication from different vendors, including Web Single Sign-On (SSO), using protocols like SAML. While this is the most adequate solution, it can be hard and time consuming to implement it.
Authentication APIs provides a fast and convenient way to add MFA to SSO web portals or home-developed applications, without the need to have deep understanding on how multi-factor authentication works.

Advantages of Cloud-Managed MFA Solutions

Cloud-based MFA provides numerous advantages over on-premises MFA solutions.

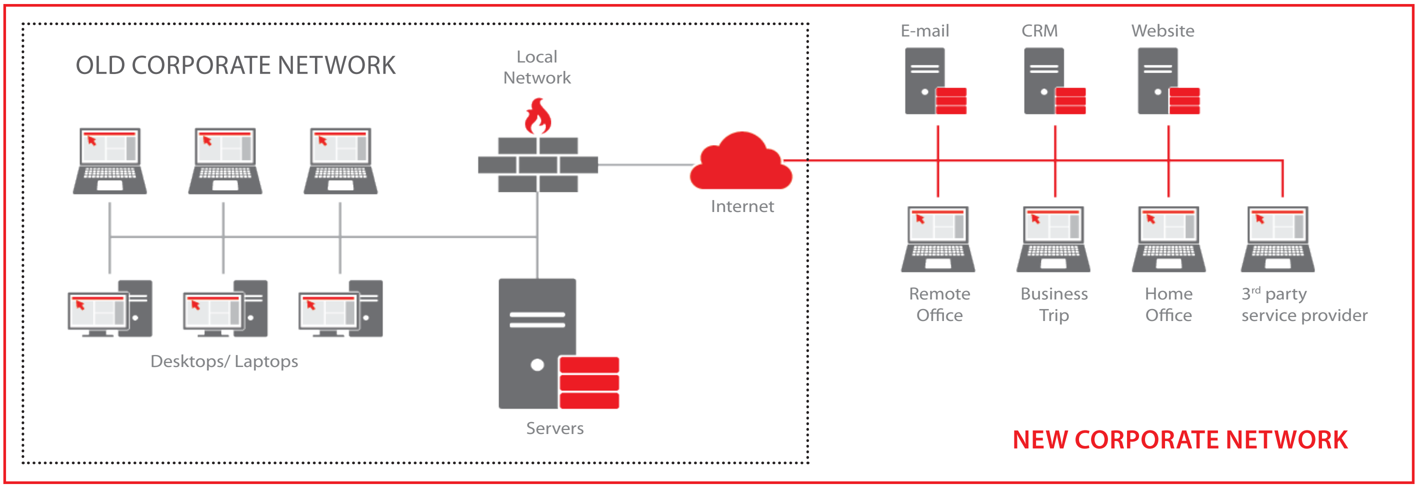
- No installation requirement
- Fast deployment
- No need to invest in hardware or operating systems
- No need to worry about patches, uptime, performance or high availability
- Everyone can manage, anywhere in the world

An on-premises authentication solution can take more than a day to set up, install and get it running. With a Cloud-based MFA, a new environment for a customer is created in less than a minute, becoming immediately available to be configured. An implementation can take less than an hour.

Remote Workforce and the Distributed Network

As previously described, the network is not just about desktops and servers connected and protected behind a firewall. The company's assets are distributed through Cloud applications, network servers, and remote computers. All of those have different users and passwords and sometimes temporary access from 3rd party service providers. This poses risks that can lead to all kinds of attacks, most of them starting with a simple username and password that could be captured, cracked, or shared through social engineering.

We are going to show how you can use WatchGuard AuthPoint solution to protect your applications with MFA.



THERE IS NO ZERO-TRUST APPROACH WITHOUT MFA

With attacks becoming more sophisticated and because extending VPN protection is not enough, businesses need to rethink their security framework to fight new and accelerated threats. In 2010, Forrester Research Inc. first coined the term "zero-trust", referring to the "never trust, always verify" security approach.

Whereas a traditional network is built around the idea of inherent trust, a zero-trust framework assumes that every device and user, on-network or off, represents a security risk. The "never trust, always verify" approach uses multiple levels of protection to prevent threats, block lateral movement and enforce granular user-access controls.

The pandemic just pushed companies of any size to adopt the zero-trust approach. Users connecting to services from anywhere, anytime, on-premises applications migrated to the Cloud – this is the perfect scenario for a micro-segmentation approach, as recommended by the zero-trust network specification.

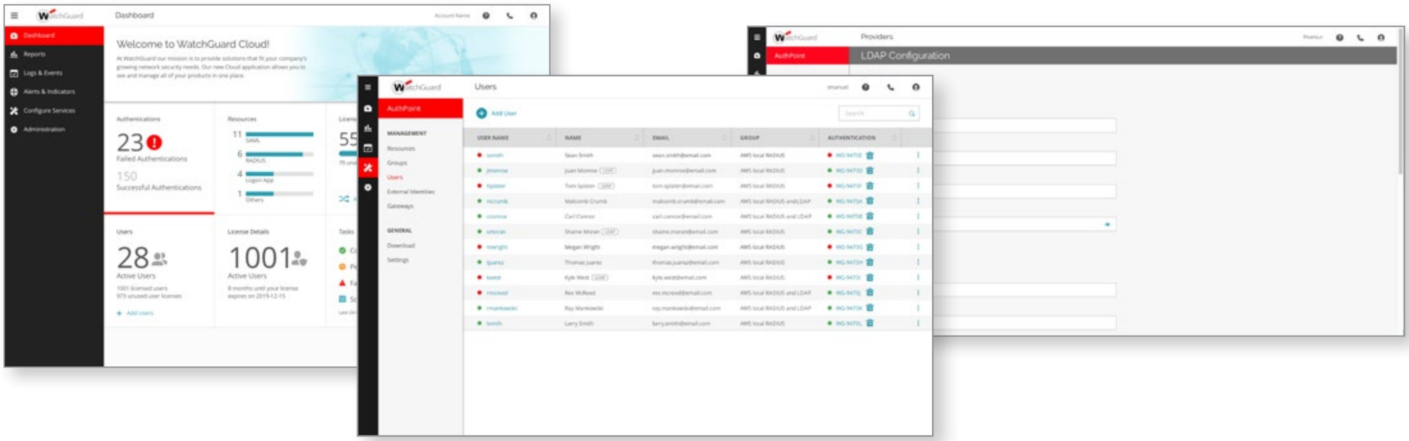
The good news is that by implementing MFA, you are taking the first step into adopting this approach. The main principles of the zero-trust framework focus on verifying user identity, devices, access, and services so no assumptions about security are made and the risk for vulnerabilities is significantly reduced.

If you are considering adopting this model, here are three key areas in the implementation of zero-trust networks:

1. **Identifying users and devices:** Always know who and what is connecting to the business network. As companies grapple with having the predominance of their workforce working remotely, securing access to internal tools presents a major challenge. Cloud-based multi-factor authentication (MFA) services offer mitigation against credential theft, fraud and phishing attacks.

2. **Providing secure access:** Limit access to business-critical systems and applications to only those devices that have explicit permission to access them. In the zero-trust framework, the goal of access management is to provide a means to centrally manage access across all common IT systems, while limiting that access to only specific users, devices, or applications. Single sign-on (SSO) technologies, combined with MFA, can improve access security and minimize the password burden on users.

3. **Continuous monitoring:** Monitor the health and security posture of the network and all managed endpoints. Malware and ransomware threats have only accelerated as a result of coronavirus. Keeping users safe as they navigate the Internet is more difficult when they are connecting from outside of your network. Staying on top of threats requires persistent, advanced security that goes beyond endpoint antivirus.



Welcome to WatchGuard Cloud!

At WatchGuard our mission is to provide solutions that fit your company's growing network security needs. Our new Cloud application allows you to see and manage all of your products in one place.

Authentications: 23 Failed Authentications; 150 Successful Authentications

Resources: 11 SAML; 6 RADIUS; 4 Logon App; 1 Others

Users: 28 Active Users; 1001 licensed users; 973 unused user licenses; + Add Users

License Details: 1001 Active Users; 8 months until your license expires on 2019-12-15

USER NAME	NAME	EMAIL	GROUP	AUTHENTICATION
ssmith	Sean Smith	sean.smith@email.com	AWS local RADIUS	WG-9473E
jmonroe	Juan Monroe LDAP	juan.monroe@email.com	AWS local RADIUS	WG-9473D
tsplater	Tom Splater LDAP	tom.splater@email.com	AWS local RADIUS	WG-9473F
mcrumb	Malcomb Crumb	malcomb.crumb@email.com	AWS local RADIUS and LDAP	WG-9473A
cconnor	Carl Connor	carl.connor@email.com	AWS local RADIUS and LDAP	WG-9473B
smoran	Shaine Moran LDAP	shaine.moran@email.com	AWS local RADIUS	WG-9473C
mwright	Megan Wright	megan.wright@email.com	AWS local RADIUS	WG-9473G
tjuarez	Thomas Juarez	thomas.juarez@email.com	AWS local RADIUS	WG-9473H
kwest	Kyle West LDAP	kyle.west@email.com	AWS local RADIUS	WG-9473I
rmcreed	Rex McReed	rex.mcreed@email.com	AWS local RADIUS and LDAP	WG-9473J
rmankowski	Roy Mankowski	roy.mankowski@email.com	AWS local RADIUS and LDAP	WG-9473K
lsmith	Larry Smith	larry.smith@email.com	AWS local RADIUS	WG-9473L

WATCHGUARD AUTHPOINT MEANS SIMPLIFIED AUTHENTICATION

WatchGuard AuthPoint was designed to provide easy-to-use, cost-effective and complete multi-factor authentication, focusing on what is really important for any business – protecting access to computers, employee credentials, networks and Cloud applications.

Some of the most recognized features of AuthPoint include optimal user experience, fast deployment and a unique mobile device DNA used to match the authorized user's phone when granting access to systems and applications.

Easy and Seamless, Above All

When compared to other MFA solutions, these are the areas that make AuthPoint powerfully easy and completely secure:

- Cloud-based: No installation of databases or servers.
- Wizards: Interactive wizards are available in WatchGuard Cloud to guide new users when configuring AuthPoint including VPN configuration, user sync from Active Directory, and more.
- AuthPoint mobile app: intuitive design, available in 13 languages that makes it user-friendly globally.
- Web single sign-on: Out-of-the-box, Cloud-based portal. Log in to all business Cloud applications using just one password.
- Documented integrations for admins and end users: Over 120 documented integrations to make it easy for admins to configure and upgrade AuthPoint.

To learn more about WatchGuard AuthPoint service, visit **www.watchguard.com/authpoint**.

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 over 18,000 security resellers and service providers to protect 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.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com