Protecting Your Network Assets with MFA

Table of Contents

THE EVOLUTION OF AUTHENTICATION – HOW DID WE GET HERE

The Authentication Problem

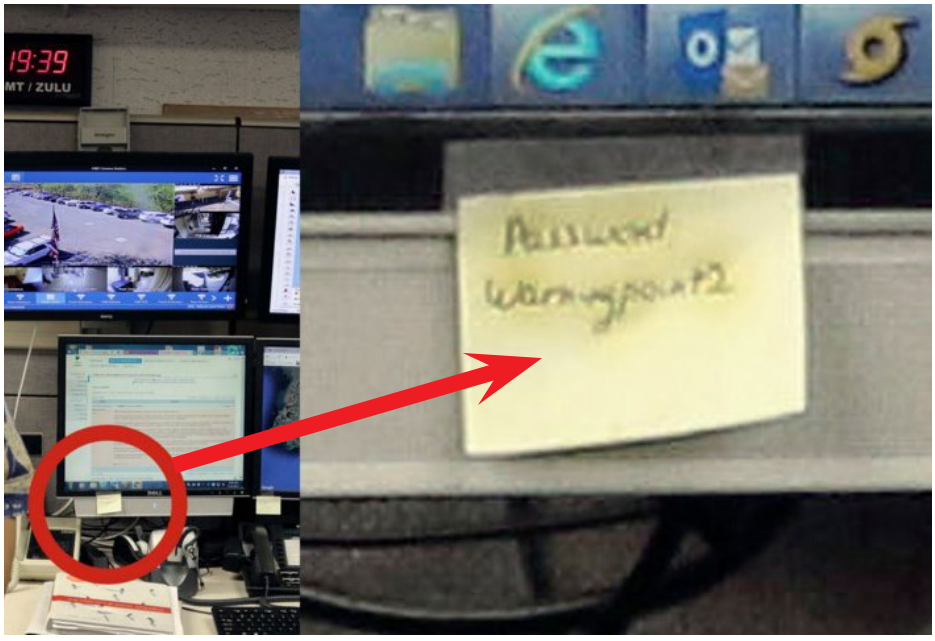
The Internet changed the way we do business. The access to fast Internet at home, as well as through millions of Wi-Fi hotspots in public places, allows employees to work from anywhere – their homes, hotels, coffee shops. Corporate information is not concentrated anymore in server rooms or data centers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



81%

of the breaches in 2016 leveraged either stolen and/or weak passwords

Verizon Data Breach Investigations

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:

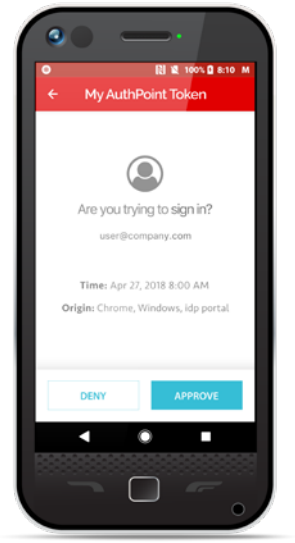
- Something you know: a password, a PIN
- Something you have: a token, a physical device, a key
- Something you are: your fingerprint, face recognition

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.

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)



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.

Security vs. User Experience

The first authenticators - or one-time password (OTP) 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!

When mobile phones finally became popular so did SMS, and SMS could now be used as a method to receive the OTP, as long as you were in a place with good service. It was not uncommon, if you were on an international trip, that you wouldn't receive your SMS, or maybe it would arrive hours later. And if you were authenticating using your phone browser, it would become a nightmare to switch between apps. In 2016, after years of experimenting with different ways to circumvent SMS-based authentication, NIST (National Institute of Standards and Technology) finally declared SMS deprecated as a two-factor authentication method.

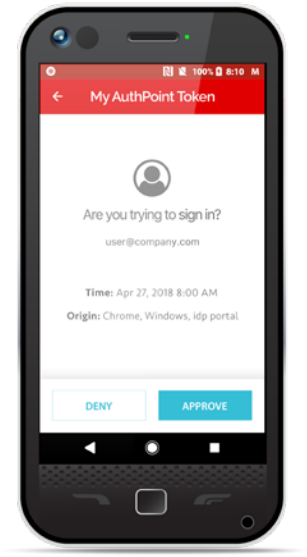
By the end of the 2000s decade, mobile phones were improving, but there were still different operating systems and vendors. Symbian, BlackBerry OS, Windows Mobile, BREW, the list goes on. Developing an app for a phone was a hard task. You needed the vendor's SDKs and had to have a collection of various 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.

> Due to the risk that **SMS** messages or **voice calls** may be **intercepted or redirected,** implementers of new systems should carefully consider alternative authenticators.
>
> *National Institute of Standards and Technology, 2016*

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.

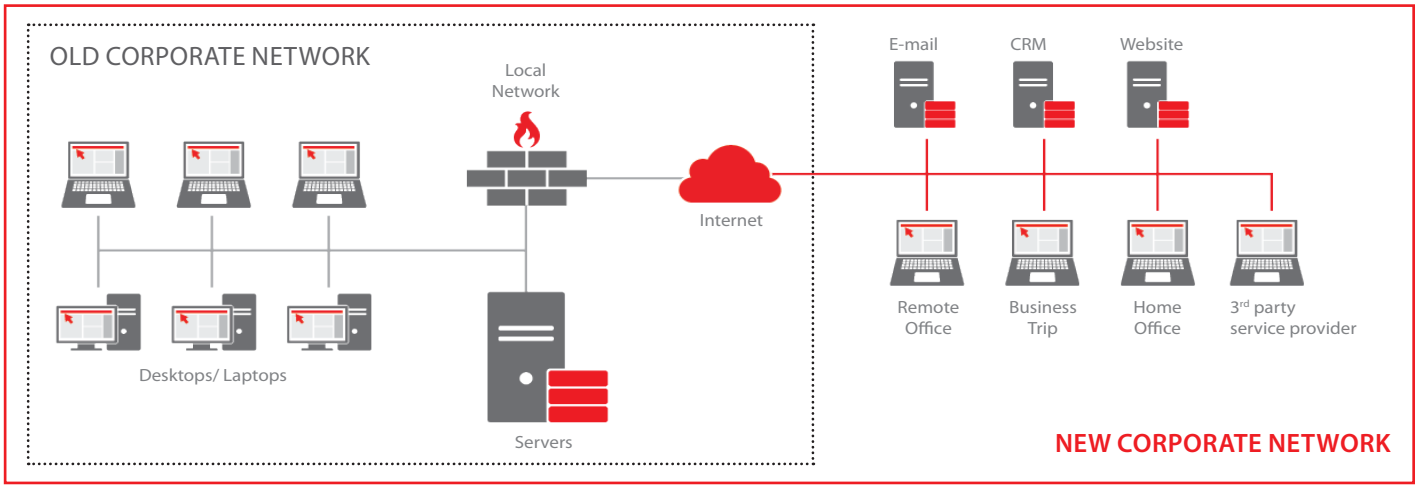
Now there is something that can provide better usability with a push-of-a-button user experience, so you know where you are authenticating to, and securely – through MFA.

PROTECTING YOUR ASSETS WITH MFA

The New Corporate Network

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.

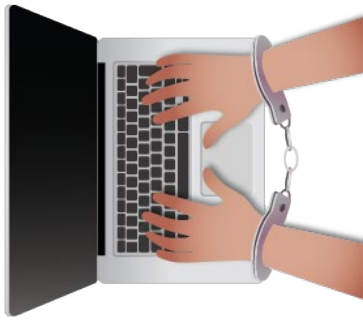


VPNs / Remote Access

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 his app, telling exactly who and where someone is trying to authenticate to. If the user is the person identified, all the user needs 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

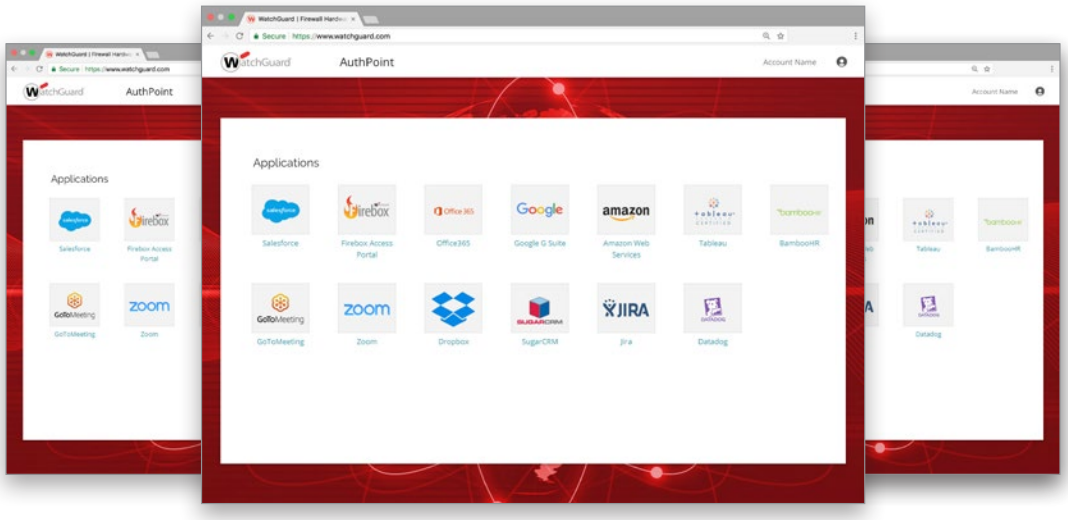
SAML (Security Assertion Markup Language) protocol was created to solve most of these issues. Its implementation is based on two main entities:

- 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

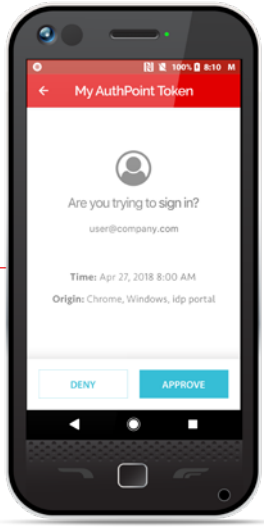
Again, user credentials can be stolen, cracked, guessed. An unattended computer can potentially be accessed by someone in possession of those credentials. This can happen on company premises, and can happen with remote or traveling employees.

The use of MFA for computer login not only protects the login process but can also provide a better user experience.

AuthPoint Logon Agent 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.

STEP 1

Click on "Send push"



STEP 2

Confirm PC Login request through AuthPoint app

STEP 3

Login is done!

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.

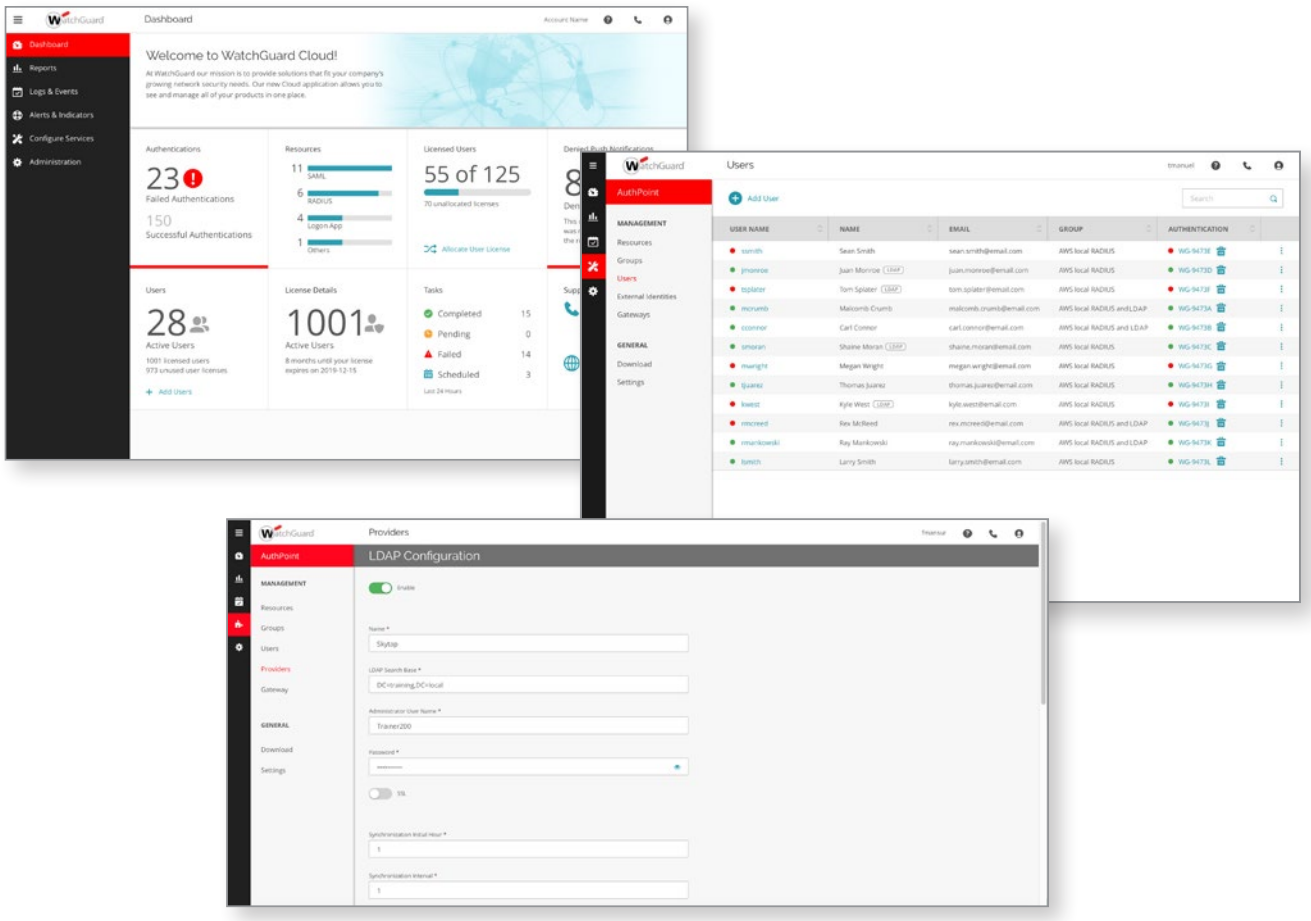
The versatility of the solution also provides a method of login into the computer when no Internet is available – the offline mode. This is important for situations such as using the laptop during a flight. In those cases, a challenge/response can be used through a QR code with encrypted data that only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

Cloud Management

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.



The Pillars of WatchGuard AuthPoint

Authentication technology has evolved to Cloud-based services, which provides fast deployment, easier integration, and worry-free management. Allied with a mobile app, the security is finally at the user's fingertips. With a single touch, the user can check and approve an authentication request, or reject an access attempt from an unauthorized intruder, blocking the cyber attack right from the start.

WatchGuard AuthPoint was designed to provide the best MFA security solution, focusing on what is really important for any business – protecting access to computers, networks and Cloud applications seamlessly, providing the best user experience.

In order to achieve that, we based AuthPoint in six main pillars:

- Security
- Simplicity
- User Experience
- Fast Deployment
- Easy Integration
- Cost Effectiveness

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

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.

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