Ping Identity®

MULTI-FACTOR AUTHENTICATION

ULTIMATE GUIDE

Ultimate Guide to Multi-factor Authentication

TABLE OF CONTENTS

CHAPTER 01

MAKE SURE YOUR USERS ARE WHO THEY SAY THEY ARE

Applications and data are becoming increasingly accessible. As we exchange and share information more often and in new ways, we're improving how we do business. But as security professionals, we're also facing new challenges when it comes to providing secure and convenient access to those who need it—while simultaneously protecting sensitive data and resources from those who don't.

It's also becoming harder to make sure your users are who they say they are. And cybercriminals and others intent on capitalizing on any vulnerability know all too well that our latest challenges represent their next opportunities.

It doesn't help that the bad actors' tried and true techniques—like phishing and other attacks that leverage weak, default or stolen passwords—are still so darn effective. The reality is that the poor password practices that have plagued enterprises for years have also remained remarkably consistent.

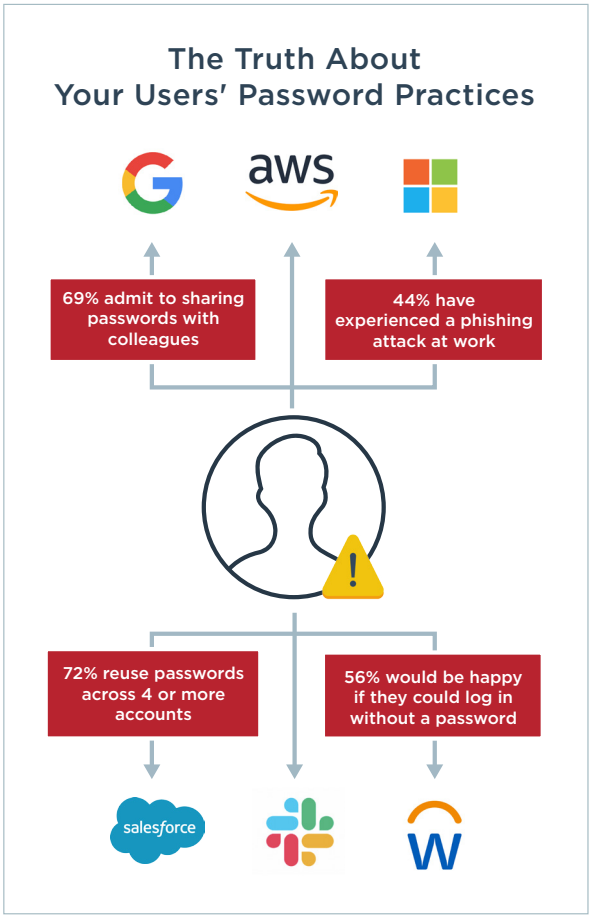
Despite knowing better, your users' password practices are still shaky at best. Your employees are likely using their work emails to register at all sorts of websites. Sometimes, they also reuse corporate passwords, share passwords with others, or even write them down. You can also assume that your customers, vendors and partners are no different.

Said plainly, if you're relying on passwords to make sure your users are who they say they are, you're putting your enterprise at undue risk.

As if cyber threats aren't enough to contend with, your customers also have higher expectations than ever about their interactions with your organization. Despite an ever-increasing threat landscape, you can't make your security measures too prohibitive or you'll face low adoption and high drop-off rates. You could even lose your most loyal customers to a competitor who's easier to work with.

Given the factors at play, striking a balance between security and experience might seem like a pipe dream. It's not. You can strengthen security and improve experience with multi-factor authentication (MFA). You know that MFA is a tried and true security method. And modern advancements in MFA remove the friction associated with legacy MFA solutions, while offering more flexibility and control than ever.

To gain a deeper understanding of how MFA works and how you can use it to increase security, let's explore five common vulnerabilities and how MFA protects against them.



How MFA Protects Against 5 Common Vulnerabilities

Defending against cyber threats can seem like an overwhelming endeavor given the number of ways that credentials could be compromised. But many successful credential thefts fall into one of five typical scenarios. And MFA is equipped to deal with all of them.

1 THE EAGER EMPLOYEE

ATTACK VECTOR: PHISHING/SPEAR PHISHING

The average phishing attack costs a mid-sized company

$1.6 MILLION.

Phishing attacks are up

65% YoY.

Employees can easily fall prey to phishing and more targeted spear-phishing attacks. Often these take the form of emails promising bonuses or rewards. All it takes is one eager employee inputting their login information to claim their so-called award for your enterprise to become the next statistic.

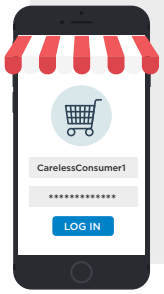
In this situation, the best offense is a strong defense. If you operate under the assumption that credentials will be stolen, you can rely on MFA to thwart the hacker's success. By requiring an additional factor to authenticate, like a mobile phone or fingerprint, MFA can stop bad actors in their tracks. And with adaptive MFA, you can step up authentication only when warranted by risk, so you don't unnecessarily impede employee productivity.

2 THE CARELESS CONSUMER

ATTACK VECTOR: ACCOUNT TAKEOVER

We all know that we're supposed to create unique logins, but doing so requires some creativity and an easy way to keep track of all of those hard-to-remember credentials. So instead, most consumers continue to use the same usernames and passwords across multiple sites—and patient hackers continue to exploit this reality using credential cracking/stuffing attacks.

While consumer adoption of MFA is notoriously difficult to achieve, you can smooth the way by embedding MFA directly into your customer-facing mobile apps. Doing so will strengthen security while also streamlining your customers' digital interactions. MFA enables the use of convenient out-of-band push authentication mechanisms like swipe, tap and biometrics. You can retire previously time-consuming and annoying processes like phone calls and password resets in favor of mobile push authentication to save customers' time and effort while also improving security.



Thieves using stolen identity credentials to launch account takeover (ATO) attacks accounted for nearly

17% of all retail login attempts.

3 THE ASTUTE ADMINISTRATOR

ATTACK VECTOR: SSH ATTACKS

SSHPsychos is so active in their brute-force attacks that at times they account for up to

35% of all SSH traffic on the internet.

Your typical employees aren't the only ones in a savvy hacker's crosshairs. Those with access to your server infrastructure are also prime targets. Secure Shell (SSH) attacks attempt to penetrate the network protocol used by sysadmins and website administrators to remotely make server-level changes. These spray-and-pray attacks attempt to use a single username and password combination across thousands of servers in hopes of getting lucky.

Adaptive MFA allows you to enforce policies for SSH logins through a pluggable authentication module or via ForceCommand. Both are proven defenses against rogue logins to Linux and Unix systems.

4 THE PERILOUS PARTNER

ATTACK VECTOR: MANY

Partners represent a similar threat landscape as your employees—only multiplied. While partnerships are an integral component of enterprise digital transformation efforts, providing third-party organizations with access to internal data expands your attack surface significantly.

But you can minimize the risks with MFA. By requiring that your partners provide an additional factor to prove they are who they claim to be, you can save perilous partners from themselves—and protect your enterprise against costly data breaches.

29% of data shared with partners

is uploaded to high-risk partners, exposing many companies to risk of data loss and breaches.

5 THE LOOTED LAPTOP

ATTACK VECTOR: PHYSICAL SECURITY

46% of survey respondents admit they have exposed themselves to laptop security threats, including:

- Leaving the laptop unattended
- Leaving the laptop in the car
- Declining regular security updates
- Attaching login information to the device
- Flying with a laptop in checked luggage

Despite your best efforts to educate and warn them of the risks, your employees may still be storing sensitive and unencrypted data on personal and corporate mobile devices for their own convenience. When devices housing sensitive data are stolen and the theft results in a breach, the impact can be significant.

You should keep providing guidance and education on secure data storage practices, but training alone isn't enough. You can use modern MFA solutions that integrate with desktop and laptop login systems to create a strong defense against this risk.

To learn more ways MFA helps you defend against vulnerabilities, read the blog.

Even if you weren't convinced before, you probably recognize the potential for one or more of these scenarios to impact your organization. Given the risks, there's little reason not to explore how MFA can help you build a stronger defense. So let's forge ahead, shall we?

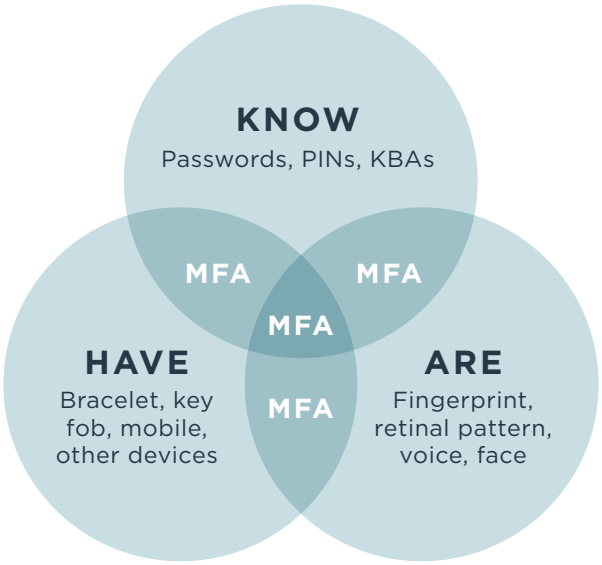
CHAPTER 02

DECONSTRUCTING MFA: EVOLUTION, AUTHENTICATION FACTORS, AND MORE

Not unlike the telephone's evolution from rotary to wireless to cellular, multi-factor authentication has continually evolved to meet changing requirements. That means today's MFA isn't your father's MFA—and that's a very good thing.

The earliest form of MFA was two-factor authentication, or 2FA. As the name suggests, 2FA required that a user provide a second factor beyond a password to prove their identity. The idea was that while a password may be easily guessed or stolen, requiring a second factor could significantly mitigate the dangers of credential reuse. And it did, proving effective at thwarting opportunistic attempts by attackers who test known username and password combinations just to see what might work.

But bad actors have gotten more sophisticated over time. And their attempts to steal credentials and compromise accounts have grown increasingly creative. Fortunately, multi-factor authentication has also advanced to address these evolving threats. But that also means that simply requiring an additional factor is no longer a sufficient defense. And just any factor won't do either. There are newer and better ways to ensure identity now, providing not just a more secure experience, but a more user-friendly one, too.



Types of Authentication Factors

In their simplest form, authentication factors are additional means of proving identity. They fall into three categories:

- Something you know
- Something you are
- Something you have

Multi-factor authentication requires you to provide two or more of these factors from different categories to prove you are who you claim to be before granting you access to your desired resource or application.

The oft-used username and password combination falls into the something-you-know category. In an attempt to increase security, some organizations might require a second something-you-know factor, such as an answer to a security question. But this isn't MFA. If fact, if a hacker were able to guess or steal your password, they could probably guess or steal the answer to your security question, too.

Instead, MFA requires that you provide factors from different categories. The idea is that a hacker may be able to guess or steal something you know, but they'll be far less likely to be able to also supply something you have, like a key card, or something you are, like a fingerprint.

IS IT MFA?

FIRST FACTOR	+ SECOND FACTOR	= RESULT
Username/password (“know”)	Security question (“know”)	NO
Username/password (“know”)	Mobile phone (“have”)	YES
Username/password (“know”)	Fingerprint (“are”)	YES
PIN (“know”)	Password (“know”)	NO
Face ID (“are”)	Token (“have”)	YES

For example, your face (through the use of facial recognition on your phone) could be an additional something-you-are factor in a basic MFA flow that starts with a username and password (a something-you-know factor). It could also be something you have, like a smart card. But the use of biometrics is understandably more popular than physical tokens as it provides a convenient way to prove identity and eliminates costly and/or burdensome hardware. Both of these benefits translate to a better user experience, as well as stronger security. And because biometrics, unlike a code or physical token, aren’t easily intercepted or stolen, you gain a greater level of assurance that a user truly is who they claim to be.

Common Authentication Factors & How to Choose Them

When it comes to authentication factors, there are a number of options to choose from, as well as considerations that apply to each. Here’s a brief overview of the most commonly used authentication factors:

Something You Know (Knowledge)

1. **Password/passphrase.** The password is the most common example of a something-you-know authentication factor.
2. **PIN.** Usually a string of 4-8 characters, the PIN (personal identification number) often requires some type of manual data entry into a smartphone, computer or other device.
3. **KBA (knowledge-based authentication).** These typically take the form of security questions, such as “What is your mother’s maiden name?” or “What was the make of your first car?”

Something You Have (Possession)

1. **Mobile phone.** Mobile phones allow users to authenticate in multiple ways, including via a mobile app or through pop-up notifications.
2. **Token.** Physical security tokens generate unique codes that only the person possessing the token can access.
3. **Key fob.** Key fobs are typically recognized through insertion in or tapping on a device, such as being placed in a USB port or next to a mobile phone.
4. **Smart card.** Smart cards contain an embedded smart chip and may be used for physical access (e.g., a room or building) or virtual access (e.g., the enterprise VPN).

Something You Are (Inheritance)

1. **Fingerprint.** Fingerprints are a popular biometric authenticator. Nearly 200 million smartphone units shipped in 2019 were equipped with fingerprint sensors, and the number is expected to grow 3X to 600 million by 2023.
2. **Facial recognition.** Apple’s FaceID feature was introduced with the iPhone X in 2017, making facial biometrics a practical, mainstream authentication option.
3. **Retinal scans and voice recognition.** Not as widely adopted as fingerprinting or facial recognition, specialty authentication factors like retinal scans and voice recognition are found in less common use cases.

When it comes to selecting the right authentication factors for your MFA deployment, it really comes down to your particular users and what makes the most sense for their needs. Here are some examples of limitations that affect authentication:

- Mobile push won't work for employees who work in call centers or clean rooms where cell phones are not allowed.
- Fingerprint authentication doesn't make sense for workers who must wear gloves to do their jobs.
- It's completely unrealistic to expect your customers to carry around hardware tokens.

Thinking about your various users' needs, behaviors and limitations will help you make strategic and sound decisions about which authentication methods to adopt. And being able to support multiple methods ensures you can serve changing and evolving use cases.

Adaptive Multi-factor Authentication

MFA as described thus far provides a greater level of assurance of user identity than simple username/password authentication. But it has its limitations, too. In its most basic form, MFA relies on a one-size-fits-all approach, requiring an additional factor regardless of situation. This can be cumbersome for users who are authenticating under typical, low-risk circumstances.

While there's no debate that MFA provides greater security than passwords alone, you can further strengthen security AND provide a more streamlined user experience with adaptive MFA. Adaptive MFA uses contextual factors and logic-based mechanisms—such as geolocation, time of day, IP address and device identifiers—to determine whether or not a user should be required to use an additional factor to authenticate.

Applying a risk-based approach to authentication requirements, adaptive authentication dynamically assesses the risk of a given operation based on:

- The user's current authentication status.
- The risk associated with the resource in question.
- The context of the request.

This risk-based approach allows you to establish policies that require an additional factor only when necessary, as determined by risk and not by default.

For example, say an American banking customer uses a password to sign on to a banking site and then tries to transfer money. If that customer signs on from the United States, the MFA system might not require further action. But if they sign on from Uzbekistan, the system could require a second authentication factor to gain a greater level of assurance that the user is who they claim to be.

Simply put, adaptive MFA provides greater control and flexibility, allowing you to strike a just-right balance between security and experience. With adaptive MFA, you can:

1. Customize authentication requirements based on risk.
2. Step security measures up or down using adaptive, contextual policies.
3. Improve productivity by minimizing authentication requirements in low-risk situations, like on trusted networks.
4. Increase security by stepping up authentication requirements in high-risk situations, like unfamiliar geolocations or high-dollar financial transactions.
5. Streamline user experience by eliminating extra steps and hardware.

Modern MFA: More than Just Adaptive Policies

Beyond adaptive policies, modern MFA provides more integrations and configurations, as well as providing more flexibility and control. With a modern MFA solution, you can:

- Protect more channels, like single sign-on, VPN, remote desktop, SSH and more.
- Provide support for more use cases, including password resets, self-enrollment, device authorization and management, transaction approvals and passwordless authentication.
- Provide support for more authentication methods.
- Lower costs by removing the need for traditional hardware tokens, SMS codes and voice calls.
- Reduce helpdesk support requirements by taking advantage of broad self-service capabilities.

See our Top 5 MFA Considerations Checklist for guidance on what to look for in an MFA solution.

Passwordless: The Future of Authentication

Passwordless authentication may seem like a radical concept, but it actually borrows from and builds upon the same principles as MFA. The basic premise remains that passwords alone aren't enough. And passwordless promises a way to bypass passwords altogether.

The elimination of usernames and passwords is also the basis of Zero Trust. In a Zero Trust environment, users are recognized and authenticated based solely on the devices used to access applications and the context in which they're attempting to access them. Sounds cool, right? But removing passwords entirely may also sound out of reach for your organization.

While going completely passwordless may not be realistic for you now, you can begin building the foundation for Zero Trust sooner than later. Reducing the use of passwords is the first step for many organizations.

You can start by leveraging adaptive MFA policies to step down authentication in low-risk scenarios. For example, you could combine a username only (no password) with a lower friction method of authentication—such as a device-based biometric (like a fingerprint) or a swipe—when a user is accessing non-sensitive resources in a typical manner (on a recognizable device and from a trusted network).

This removes friction from the end user experience, and is a good first step. But if you still require passwords in some situations, those passwords are still vulnerable to reuse, theft and subsequent use by a bad actor.

More advanced organizations are adopting standards such as FIDO2 which remove passwords altogether. Instead of passwords, FIDO2 leverages public key cryptography methods that require users to register a device and a domain (e.g., a corporate email) from which future access requests will originate.

While you may not feel ready for this, you may be more ready to start your journey to passwordless authentication than you realize.

Learn more about passwordless authentication.

CHAPTER 03

BENEFITS OF ADAPTIVE MFA

Striking a balance between security and experience isn't easy. But it's exactly what adaptive MFA was made for.

Reduced Risk of Breach

Using MFA makes it more difficult for hackers to steal credentials or use brute force to breach your systems. Given the magnitude of costs associated with a typical breach—including the lost revenue and damage to your company's reputation—proactively reducing your risk of breach can have a substantial impact on your top and bottom lines.

Adaptive MFA extends beyond the basic multi-factor authentication protocol to apply authentication requirements based on the risk involved in the requested access. If the risk is low—such as accessing non-sensitive resources from a recognized device—you can require minimal authentication requirements. On the other hand, if the risk is high—like a money transfer request made from a foreign location—you can set policies to require additional authentication.

> "IT and security professionals consider multi-factor authentication to be the most effective security control they have in palce for protecting both on-premises and public cloud data."
>
> - The State of Enterprise IT Infrasctructure & Security, 2018

Improved User Experience

Because adaptive MFA allows you to dynamically step authentication requirements up or down, it delivers a better, more streamlined experience for legitimate users. If a user is performing a routine transaction or making a routine request, they'll have the seamless experience they expect. And if they're attempting something more sensitive or risky, they'll be prompted for additional authentication that provides security reassurance.

Adaptive risk-based MFA is the key to delivering a frictionless and consistent user experience. You're able to strengthen security only as warranted, stepping up authentication requirements for high-risk access and reducing them for low-risk access. Users exhibiting safe and predictable patterns of use—arguably the vast majority of your access requests—are able to quickly and easily access resources.

MFA + SSO: How to Increase Productivity & Reduce Administrative Costs

MFA improves security by requiring users to provide additional information to prove they are who they claim to be. At the same time, adaptive MFA improves experience by adapting authentication requirements to the situation instead of requiring a one-size-fits-all approach.

While MFA minimizes reliance on password authentication alone, it doesn't address the root problem of password sprawl. Your users are expected to create, remember and manage a growing number of passwords, numbering in the dozens if not hundreds for the average user. Their password fatigue is a large part of why their passwords are weak in the first place.

The issues with passwords don't end there either. It's estimated that the average employee spends 12.6 minutes each week or 10.9 hours per year entering and/or resetting passwords[1]. This may seem insignificant on an individual level, but when you do the math across an organization of, say, 500 employees, the loss of productivity is a six-figure problem. If your organization is bigger than around 3,000, you can add another zero.

You can overcome this costly problem while also improving security and experience with single sign-on (SSO). SSO allows users to sign on once using a single set of credentials and gain one-click access to applications. Your users—whether employees, customers, or both—no longer have to manage or enter multiple passwords, streamlining their experience and saving time.

Fewer passwords is better for your IT team, too. By reducing the number of passwords in use, you significantly reduce the number of password reset requests you need to manage. This frees up your helpdesk to focus on more pressing priorities and high-value initiatives.

When you implement MFA and SSO, you drastically reduce the number of passwords in play and provide an additional layer of protection for the "one" password that remains. MFA combined with SSO helps you:

- Increase employee productivity by reducing time spent logging into applications.
- Improve security by mitigating password sprawl, eliminating poor password hygiene and curtailing reliance on password vaulting.
- Reduce password reset requests and their associated costs.
- Respond to BYOD and mobile access demands.

1 The 2019 State of Password and Authentication Security Behaviors Report, Ponemon Institute

CHAPTER 04

USE CASES FOR ADAPTIVE MFA

Adaptive MFA is ideal when your use cases have expanded outside the traditional firewall to include both managed and unmanaged devices, as well as on-premises and cloud apps. As digital transformation and other modernization initiatives require that you provide increased access to confidential information, you need a more sophisticated approach to authentication.

Of course, this is the new reality for most if not all organizations, so adaptive MFA is often applicable across the user spectrum—from your workforce to your customers to your partners—and a range of industry verticals.

Workforce: Improved Security & Productivity

It's an understatement to say that managing access for today's workforce is more complex than it used to be. Beyond typical employees, many organizations must extend access to other workforce-related users, including independent contractors, subcontractors, franchisees and the list goes on. Adding to this complexity, employees and other "internal users" are often externally located, making the focus on perimeter-based security a relic of the past.

Adaptive MFA makes it easier to extend secure access to these users by allowing them to access resources from any location and any device, as well as gain access to all applications and APIs, whether on-premises, SaaS-delivered or in public or private clouds. By enabling access from anywhere, adaptive MFA allows your users to work from anywhere—and be more productive. And because it's adaptive based on context, legitimate users exhibiting typical behaviors gain quicker and easier access to resources, improving productivity and experience.

Because remote workforce access was the primary driver for MFA adoption in the enterprise, out-of-the-box integration with popular VPN solutions remains a common requirement. But many of today's enterprise resources are hosted outside of the firewall, and the proliferation of stolen credentials as an attack vector is driving CISO-level initiatives to implement MFA everywhere.

Everywhere is a broad term, but enterprise considerations should include common and emerging use cases, and the out-of-the-box integrations that coincide with faster time to value. You can use modern MFA to protect traditional web applications, as well as additional resources and the channels used to access them, like:

- VPN access
- Web SSO
- Remote desktop
- Privileged access
- Workstation and network login

Learn more about improving productivity and usability for your digital enterprise with MFA.

Customers: Better Experience

Regardless of whether you're a household brand name or a B2B provider, your customers want to interact with your organization online and across multiple channels. In response, you must provide the secure access and consistent experiences they've come to expect. If the authentication process is inconsistent, inconvenient or overly persistent, your customers can become frustrated and opt out.

Adaptive MFA as part of a customer identity and access management (IAM) approach provides a consistent and strong authentication experience regardless of the channel customers use to interact with your business. You can set policies to require second authentication factors (such as SMS or biometrics on a mobile device) based on an assessment of contextual or transactional risks. You can also integrate MFA functionality directly into your own customer-facing mobile app. Embedding adaptive MFA into your existing mobile application can further increase both convenience and security for customers.

Typical use cases for customer MFA include:

- Password resets
- Device authorization and management
- Website sign-on
- Transaction approval
- Passwordless authentication
- Identity confirmation

Learn more about how MFA helps you personalize and streamline customer experience.

Partners: Secure Access

Providing access to partners is yet another reality for many organizations. But between managing varying levels of access and accommodating your partners' identity and access management (IAM) capabilities, enabling that access securely and conveniently can feel like a tall if not impossible order. What's more, you don't have access to HR information to guide the enabling and disabling of access privileges, leaving the potential for a former partner employee to maintain access to your resources.

Like with other uses case, adaptive MFA allows you to set and enforce policies to address the diverse requirements of providing partner access. When you implement adaptive MFA for partners in combination with single sign-on (SSO), you can also streamline partner onboarding, while eliminating the headaches of managing partner password resets and avoiding the risks of managing partner identities.

Learn more about simplifying partner identity and access management with MFA.

Federation: Connect Any User on Any Device to Any Application

Today's modern enterprises serve multiple different identity types, from workforce to customers to partners. This complex ecosystem is most effectively managed by identity federation, which provides a bridge to connect all of those different user identities in one place and reduces your administrative overhead. A versatile federation solution can solve your current and future identity management challenges. As your organization evolves to allow more users to securely access the applications they need, a single authentication authority will be essential.

Learn more about federation.

Industry Applications for Adaptive MFA

Adaptive MFA provides advantages for a number of industry verticals, including but not limited to financial services, retail and healthcare.

Financial Services: Protect High-Risk Scenarios & Achieve Regulatory Compliance

As the keepers of such valuable information as social security numbers, online banking credentials, financial account info, mortgage terms and insurance details, financial services organizations are a prime target for hackers. But customers still want to be able to access their accounts and make transactions quickly and easily.

Adaptive MFA is a perfect fit for the financial industry, providing a comfortable sense of security for customers in high-risk situations like during high-value transactions or large-volume transfers, while allowing low-risk activities to continue without interruption.

Strong multi-factor authentication also helps financial organizations satisfy regulatory requirements like Open Banking in the UK, Europe and Australia, which opens third-party access to consumer data in a secure manner, and New York's 23 NYCRR 500, which addresses the heightened risk of cybersecurity threats in the financial services industry. LEARN MORE

Retail: Provide Frictionless & Consistent Customer Experiences

As retail becomes increasingly cutthroat (often called the Amazon Effect), retailers are looking to digital innovation to maintain a competitive advantage. New retail channels and digital properties provide new ways to gain customer affinity and loyalty. But they also require more security. While MFA can provide the security retailers need, it traditionally added friction to the customer experience. And nothing will kill competitive advantage quicker.

MFA is your best defense against compromised customer credentials. It's even required in regulatory requirements such as PCI DSS. But beyond security, modern MFA also realizes that you can't prioritize security over customer experience. Adaptive MFA enables you to strike the perfect balance and ensure secure, convenient and seamless customer transactions. LEARN MORE

Healthcare: Improve Experience without Compromising Security

To differentiate themselves, market leading healthcare organizations are investing in improved experiences across their networks. But as updated facilities and patient personalization become table stakes, payers and providers must seek out unique ways to delight their patients and members across the spectrum of care.

Whether they're ordering a no-foam triple grande latte or seeking a dermatologist to do a skin-cancer exam, today's consumers have high expectations about the convenience and consistency of their digital interactions. In addition to securing PII and PHI, modern MFA allows you to improve healthcare experience by offering modernized communication methods, convenient ways to verify identity, improved access to online resources and the ability to quickly provide health data access to third parties. LEARN MORE

CHAPTER 05

HOW ADAPTIVE MFA WORKS

For the Administrator

Adaptive MFA works in the background to develop an active assessment of the user. This might include contextual, behavioral or correlative factors, including the geolocation, computing environment and nature of the transaction being attempted. If policy surrounding any of these factors dictates greater security, the system can step up authentication requirements to apply the correct level of security based on the associated risk.

As an administrator, you set access control policies to dictate the need for strong multi-factor authentication. Since these policies are based on risk, you'll typically start with a data classification exercise that identifies your audit risks, as well as the data that's most at risk should your organization be compromised (PII, PHI, credit card numbers, social security numbers, intellectual property, etc).

You will then map the users, devices, applications and APIs able to access your sensitive data and determine the level of acceptable risk in certain scenarios, identifying those that:

- Don't require MFA
- Require some form of MFA
- Require high assurance and a specific form of MFA
- Warrant a denial of user access, because MFA isn't enough to overcome the risk

Armed with this information and understanding of your risk profile, you're able to set security policies in line with the risks associated with specific resources, behaviors and contextual factors.

Is There an Easier Way to Implement MFA?

If data classification exercises and user maps sound more complicated than you need or want to take on, not to worry. Modern MFA solutions are:

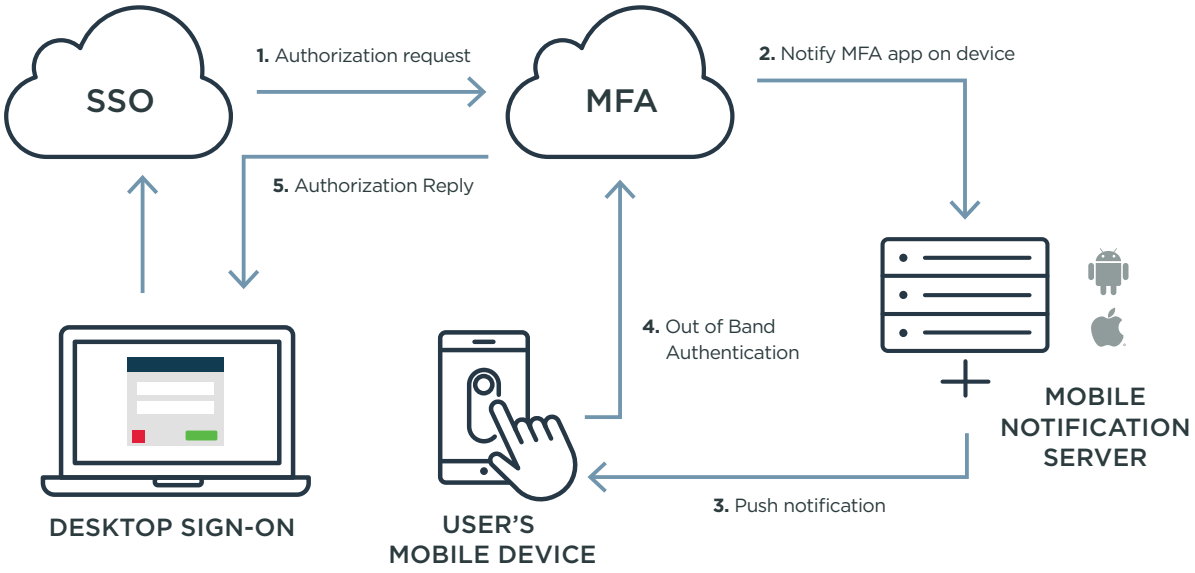
- Fast to implement
- Simple and convenient for users to adopt
- Fit within your IT budget
- Can easily grow with your company's changing security needs

Learn more about MFA made easy.

For the End User

Adaptive MFA enables users to securely and conveniently authenticate to all of their applications. They simply install an app on their phone and self-register that device. The app may be a standalone MFA app for authentication purposes only. Or you can embed MFA capabilities in your own app, which is often more convenient for customer end users. Regardless of how you implement, adaptive MFA is easy to set up and use, while providing strong authentication to all of the apps your users need to access.

When your governance policies dictate the need for strong authentication, the MFA service sends a notification to the user's smartphone. If the user employs iOS or Android devices, the Apple or Android notification service sends this notification. This eliminates the cost of a voice call or SMS message. Upon receiving the notification, the user swipes his or her device to sign-on and is authenticated.



If a user can't get online but needs access to their device, offline modes can generate a one-time passcode (OTP). Alternatively, SMS, voice, email or a desktop application can deliver the OTP. YubiKey and other hard tokens can also be employed for sensitive environments or for users without mobile device or phone access.

Watch the video to see MFA in action.

CHAPTER 06

IMPROVE SECURITY & EXPERIENCE WITH ADAPTIVE MFA

The beauty of adaptive MFA lies in its inherent security and flexibility. Because security requirements are rarely cut and dried, a one-size-fits-all solution just won't work. Some situations call for greater security, such as high-value transactions on untrusted networks and devices. While other situations fall under safe and predictable use, making additional security measures prohibitive and unnecessary.

Adaptive MFA provides the ultimate in flexibility, allowing you to control the level of security based on your specific risks and requirements. You can add authentication factors and gain a higher level of assurance about a user's identity when conditions warrant it. Or you can provide streamlined access for a user that demonstrates safe and consistent patterns. You can even use stronger authentication methods like mobile push authentication, QR codes and FIDO-compliant authenticators instead of credentials to enable passwordless authentication.

Want to provide the best of both worlds when it comes to security and experience?

LEARN MORE ABOUT MFA

#3150 | 12.19 | v001