BEYOND IDENTITY

The Next Frontier of Multi-Factor Authentication

Securing device-based access

Contents

Executive Summary

Passwords are the most common attack vector and are a leading cause of data breaches.[1] Companies turned to multi-factor authentication (MFA) for a more robust alternative to basic passwords to increase assurance of a user's identity at authentication. However, since most MFA solutions rely on passwords as an authentication factor, password-based MFA remains equally vulnerable to password-related attacks such as phishing, man-in-the-middle attacks, SIM swaps, and more.[2] Today, more than 80% of cyberattacks start from stolen or leaked passwords.[3] Hence, it is no longer enough to simply rely on password-based MFA.

Organizations need to be able to verify the identity of users with confidence. The workforce is using more devices, both managed and unmanaged, from different locations at a rate faster than companies can identify and secure. Enterprise software-as-a-service (SaaS) apps can be accessed from anywhere, on any device. There's no way to control access and protect company data. Increased prevalence of SaaS apps, bring your own device (BYOD) policies, and a historic rise in remote work[4] is fading the security perimeters of organizations. The inherent weakness of password-based MFA fails to keep up with these evolving security requirements of modern work environments.

Companies must reinforce how they authenticate users in today's SaaS-dominant world to protect company data. MFA must meet the new requirements of the modern workforce. This white paper examines what CISOs and IT leaders should expect from a truly secure MFA solution for modern work environments by evaluating the main objectives of MFA.

The emergence of MFA

Today, security leaders know that passwords are a fast-growing attack vector. In 2020, 94% of enterprises were impacted by at least one password-related breach.[5] To mitigate credential threats, MFA emerged as the de-facto authentication standard.

MFA grants access based on two or more factors:

- Something you know, such as passwords and knowledge-based questions
- Something you have, such as a mobile device, key fob, or CAC card
- Something you are, such as fingerprints, iris scans, or some other biometric data

When MFA first emerged, companies used MFA mainly to strengthen authentication to enterprise applications primarily deployed on-premises. Employees accessed those apps only from company-managed devices. Typically, users had to be on campus to connect to systems in the company's private networks and on-premise data centers. User and device-based access controls were much simpler back then than the current cloud-driven ecosystem.

Among several early variants of MFA was RSA's SecureID, commercially launched as a key fob in 1986.[6] RSA's key fob is external hardware with a small LCD screen displaying a one-time password (OTP)

[1.] https://www.ibm.com/security/data-breach
[2] https://www.beyondidentity.com/blog/how-your-mfa-can-be-hacked-examples
[3] https://www.beyondidentity.com/blog/5-key-takeaways-2021-verizon-data-breach-investigations-report-dbir
[4] https://www.oberlo.com/blog/remote-work-statistics
[5] https://www.forbes.com/sites/louiscolumbus/2020/09/06/the-state-of-identity-security-2020/?sh=181023b43f36

that refreshes itself every 60 seconds. When users requested access to a network or company resource, they'd enter their password, then the OTP. After 60 seconds, that OTP would time out, and users would need to input the new OTP. Both government and corporate users adopted RSA SecureID. Its popularity underpinned the usage of an authentication factor tied to a user's possession of "something you have" (key fob) for the first time.

Decades later, the advent of smartphones quickened MFA adoption as companies could then leverage users' existing devices as the second factor. Duo, for example, asked users to verify their identity by inputting a password and then picking up the Duo mobile app and approving push notifications before accessing applications. However, the Due app was portable. Users could authenticate on any other computer or device using their phone, exposing organizations to device-related vulnerabilities.

Moreover, in all of these MFA solutions, passwords remained the first authentication factor.

At the 2004 RSA Conference, Bill Gates declared the password dead.[7] Yet here we are today, with users managing dozens to hundreds of different passwords, which leave organizations vulnerable to password-based attacks.

Password-based MFA is prone to attacks

Most MFA solutions add an authentication factor to the password as one more layer of defense. While this reduces some risk, the password remains the weak link. Often, MFA also uses weak factors such as SMS text messages or OTPs that are easily phishable. Listed below are common attack vectors on password-based MFA.

Attacks on passwords

Centrally managed passwords like password databases create a "honeypot" for attackers. Incidents involving massive password leaks from multiple databases are now increasingly common.[8] The cost of password-related breaches is significant. In 2021, compromised passwords accounted for 20% of breaches at an average cost of $4.37 million.[9] The Colonial Pipeline ransomware attack, which cost the company $2 million in ransom, began with one stolen password.[10]

[6] https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-2-offering-two-factor-authentication/

[7] https://www.cnet.com/tech/services-and-software/gates-predicts-death-of-the-password/

[8] https://techxplore.com/news/2021-06-largest-password-breach-history-leaked.html

[9] https://www.ibm.com/security/data-breach

[10] https://www.forbes.com/sites/forbestechcouncil/2021/09/14/one-stolen-password-took-down-the-colonial-pipeline---is-your-business-next/?sh=1a81c1635f56

Risks with authentication factors

Something the user **knows**	Something the user **has**	Something the user **is**
Knowledge-based factors include passwords, security questions, one-time codes via email, etc. Common risks: · Easily reused, shared, stolen, and compromised · Passwords have been one of the top two causes of data breaches over the last decade	Possession factors are commonly used in MFA solutions and include SMS text messages, OTPs, mobile phones, key fobs, etc. Common risks: · Delivery mechanisms such as emails and SMS can be easily intercepted · External hardware fobs can be easily stolen or lost · SIM swap to intercept SMS codes	Biometric characteristics such as face ID and fingerprints are challenging to imitate. However, where biometric data is stored is crucial to how you measure the trustworthiness of this authentication method. Common risks: · Biometric data is really sensitive and cannot be changed · When stored in databases, creates a honeypot for attackers

Attacks caused by phishing emails

Companies often adopt MFA to respond to phishing attacks luring users to release their passwords. However, phishing attacks can be just as effective[11] against organizations using MFA as those without. When using MFA, the only difference is hackers now have to phish one additional password or PIN, which they often easily accomplish. For example, they can spoof the landing page that requests the confirmation code and then enter it on the back end to the actual landing page.[12] In many incidents, the hackers manipulate customer service agents into releasing credentials and other information, which are subsequently used to compromise user accounts.

SIM swaps bypass the second factor

SIM swapping techniques allow hackers to turn their phones into yours. To install your number in their SIM, all it requires is a call to the phone company and a bit of social engineering. They don't even have to be on the same continent as you to steal your phone. SIM swaps allow the second authentication factor to be sent directly[13] to the hackers, entirely bypassing you in the authentication flow.

Man-in-the-middle attack to steal your session

In a man-in-the-middle attack, the hacker places a proxy between the client and the server, intercepting everything the user types until the access token is granted in the MFA sequence. Once access is granted, the hacker enters undetected—a scheme called session hijacking.[14]

[11] https://www.zdnet.com/article/hacker-spoofing-bypasses-two-factor-authentication-security-in-gmail-secure-email-services/
[12] https://www.techrepublic.com/article/how-a-phishing-attack-thwarted-mfa-to-steal-money-from-coinbase-customers/
[13] https://www.zdnet.com/article/fbi-warns-about-attacks-that-bypass-multi-factor-authentication-mfa/
[14] https://www.theregister.com/2011/05/27/lockheed_securid_hack_flap/

> "Though widely used, passwords are fundamentally flawed and no longer an appropriate authentication method for any use case except those with minimal risk." [15]
>
> – Ant Allan, VP Analyst, Gartner

Man-in-the-endpoint attack bypassing MFA

Hackers can bypass MFA by installing malware on the device endpoint. This malware is engineered to start rogue sessions in the background after the user authenticates. Its fallout can be substantial. For example, suppose hackers employ the malware to create a hidden session when an employee logs into the corporate HR platform. In that case, they can easily steal the employee's identity data to manipulate bank accounts and other financial transactions.

Rebuilding the passcode generator

The OTPs generated by MFA solutions are often created by an algorithm based on a seed number. Although one of the more complicated methods, hackers have been able to reverse engineer these algorithms and seed numbers to generate the one-time codes accurately. It's equivalent to measuring a keyhole to build a key that will unlock it. The high-profile breach of Lockheed Martin[16] is a testimony to how hackers reverse-engineered the MFA algorithm after compromising the seed value used to generate RSA SecureID tokens.

Usability challenges affect MFA compliance and adoption

Even though MFA emerged as the "go-to" defense against unauthorized access, password-based MFA has much lower adoption rates than firewalls, endpoint security, and email protection. Password-based MFA has become more than a mere annoyance, particularly in the workforce, as users often need to access five, ten, or more applications daily. When MFA is difficult to use, users will do everything to avoid complying.

When MFA requires users to enter a password, users spend a lot of time creating passwords, resetting them frequently, locating a secondary device (their phone or a fob), and entering one-time codes or answering push notifications. These elements collectively degrade the user experience, negatively impact organizational productivity, and seriously hinder MFA adoption.

Users do everything they can to avoid using MFA and even abandon logging into certain resources if the barrier to entry is too high. This impacts identity and security architects, who compromise on security policies to keep their workforce satisfied and productive.

Some organizations end up using MFA only for a few select apps. Another frequent tradeoff is to increase application session timeouts from hours to days, or even months, leaving applications open to session hijacking attacks.

[15] Ant Allan, Gartner "Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls" April 4, 2019.

[16] https://www.theregister.com/2011/05/27/lockheed_securid_hack_flap/

PSST! Hey, Your Users Hate Passwords and MFA

From Salesforce to Bank of America, many business and consumer-oriented platforms use password-based MFA. Yet the inconvenience and insecurity of passwords, along with the friction caused by numerous steps and devices, persists today.

- Only an estimated 11% of enterprise cloud users have adopted password-based MFA, even though MFA[17] was the top security technology chosen due to global shifts to work from home in response to COVID-19[18]
- Of those who have not adopted, 43% have blamed the clunky user experience as the reason[19] and 41% cited complexity as the reason

Evolution of scalable, high-assurance authentication methods

MFA had to rely on passwords due to the absence of scalable, high-assurance authentication methods. Historically, high-assurance authentication methods either required complicated infrastructure to support them—whether physical infrastructure, such as CAC readers, or digital infrastructure, such as Public Key Infrastructures (PKI) and centrally managed certificate authorities. These options were impossible to scale for thousands of users and devices at mid-to-large size organizations, and, even after set up, they were time consuming and costly to manage. But that's changing.

Today, three recent technology advances in hardware and infrastructure have positively impacted how companies can use scalable, high-assurance authentication factors everyday for their workforce:

- Trusted Platform Modules (TPMs): TPMs (also referred to as the "secure enclave" in Apple devices) provide hardware components that serve as a secure storage mechanism for security artifacts and verifies that your device is functioning properly and is trustworthy. Introduced in the late 2010s on almost all modern computers, tablets, and phones, they offer a safe place to generate and store cryptographic keys locally on the hardware of each device.
- Biometric readers: Most modern devices now have biometric readers built in so users no longer have to use external fingerprint or Face ID cameras to authenticate to their device which makes it nearly impossible for anyone but the owner to access the device's contents.
- The emergence of FIDO: The FIDO Authentication framework enables widespread adoption of private/public key cryptography-based authentication across websites and applications. Committed to ending the use of passwords, FIDO's open standards framework asks a user's device to create a new key pair and retains the private key on that device. Then, when a service challenges the user's device, the private key on the device

[17] https://blog.systemsengineering.com/blog/new-statistics-warn-about-the-urgent-need-for-mfa
[18] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets
[19] https://www.yubico.com/blog/75-of-enterprise-security-managers-plan-to-increase-mfa-spending-according-to-new-study-by-yubico-and-451-research/

issues a public key to prove possession. These open standards have paved the way for public/private key cryptography to be used in a frictionless way for everyone.

These technologies enable authentication methods with a higher-assurance level to verify the identity of users because:

- With widespread adoption of FIDO standards-based public/private key cryptography on users' devices, organizations no longer need to create a full PKI infrastructure.
- When keys are generated and stored in the TPM, users don't need to manage their own keys.
- TPMs are a really secure place to generate and store keys because the TPM stores platform data to let you know whether it's been altered or compromised.
- Devices can store biometric data locally in the TPM so companies no longer need to securely store users' biometric data in their databases (which is highly sensitive and can't be changed).
- Local PINs to access the device are protected by anti-hammering—the device only allows a set number of login attempts before locking or wiping the device.

These recent technologies have paved the way for higher-assurance authentication methods to be used at scale for organizations of all sizes. It's a step in the right direction but then the challenge becomes: how do you support your workforce across all of their authentication use cases and device types?

MFA today must identify the user and the device

In a SaaS-first world, anyone with a password can login to any device. With the increase of remote work, BYOD continues to rise. More employees are onboarding remotely, there are reduced budgets for corporate-issued devices, and there is a lack of time and resources to continuously support a company-wide mobile device management (MDM) program. (Plus, employees may not want to add an intrusive MDM solution on their personal phone anyways.)

This results in more devices accessing SaaS resources at a faster rate than organizations can identify and secure them. Protecting against highly risky authentications on these insecure, non-company issued devices is a top priority.

This creates a challenge for IT and security teams: how do they set up device-based access controls for SaaS resources to ensure that only authorized users and secure devices can login to BYOD devices to ensure endpoint security, all without impacting the flexibility and productivity of the workforce?

If the goal for organizations is to be able to identify each user behind the device, and decide whether that device should be granted access, teams will need to start asking questions such as:

1. Is this device tied to an authorized user?
2. Is this device registered in our directory?
3. Does it have company-issued apps and software on it (i.e., MDM, EDR, VPN, etc)?
4. Is it jailbroken?
5. Does it have a biometric enabled?
6. Is antivirus software running?
7. Does it have the bare minimum security requirements to gain access?

In addition to strong factors, MFA must also keep up with the needs of the modern workforce who are accessing company resources on company-issued and personal devices. Today, most password-based MFA solutions allow users to use a "roaming" authenticator mobile app to login on whatever computer, tablet, or phone they want to get access from. They could access company resources on an insecure shared computer at the library or a hotel and the IT and security team would be powerless to stop it. MFA should take into account different high-risk authentication use cases to verify the identity of the user, and if the user should get access on that device.

> **MFA is the best defense against unauthorized access only if it:**
>
> - Eliminates passwords, and their vulnerabilities, from the authentication workflow
> - Establishes device trust for every device accessing resources or attesting for identity

Conclusion

MFA is no longer about keeping passwords and adding OTPs and push notifications in a SaaS-dominated world. Device-level threats like malware, poor patching, and misconfigurations place organizations and users at risk every day. MFA must verify the user's identity with confidence and guard your organization against account takeovers and data breaches. The best solution is to ensure that the device that is accessing the SaaS resources is bound to a user, and that the device is secure enough to access company resources. This is only possible by replacing passwords with stronger, more secure factors. One of the most robust forms of authenticating users is device-level biometrics, cryptographic keys, and checking the security posture of every device requesting access to your apps and resources. A truly secure passwordless MFA is device-based that promotes adoption and compliance while reducing friction for users.

About Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in—eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.

Ready to Have Beyond Identity Solve Your Authentication Challenges?

GET A DEMO

beyondidentity.com | info@beyondidentity.com

BEYOND
IDENTITY