Risk Assessment: Multi-Factor Authentication (MFA) Security

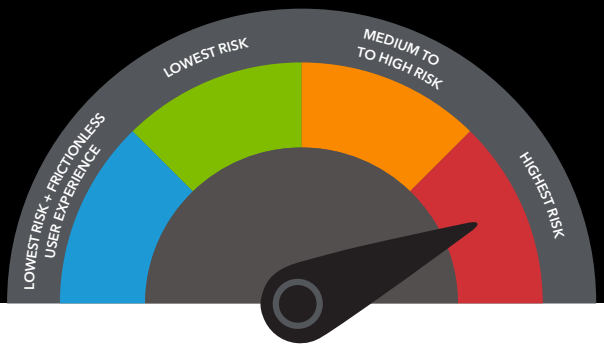
Understand the Risk Scale of Today's Authentication Solutions

Eighty percent of all hacking-related breaches involve stolen user credentials or poor password hygiene,[1] and more than 613 million passwords have been exposed through data breaches.[2] Adding multi-factor authentication (MFA) as an additional login security layer can significantly reduce risk, but most traditional MFA solutions can still be compromised with relative ease.

How mature is your organization's authentication security? Understand the risks of today's authentication models:

Highest Risk

Username and password authentication



Organizations that rely solely on credential strength for secure authentication are highly vulnerable to attack. Usernames and passwords are less secure than ever before. Login details are stolen, hacked, and harvested by highly motivated actors, then quickly monetized – used or sold on the dark web.

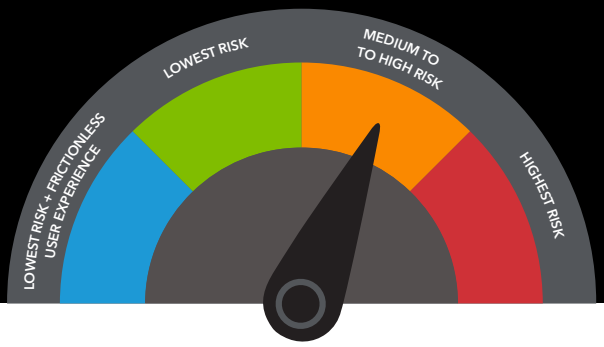
How malicious actors bypass usernames and passwords:

- **Credential stuffing**
- **Phishing**
- **Password spraying**
- **Brute force**
- **Prior data breach / reused passwords**
- **Password reset**
- **Keystroke logging**
- **Local discovery**

And the fact that users tend to repeat passwords across multiple sites further threatens enterprise security; you're only as secure as your users' least secure personal account. The vulnerabilities inherent to even the most complex, algorithm-generated passwords prove the need for MFA. Ultimately, it is never advisable to rely on one level of security – single-factor authentication in this case. Best-in-class security always includes multiple layers of defense.

Medium to High Risk

Standard multi-factor authentication (MFA)



Adding MFA functionality to your authentication security stack immediately improves enterprise security. MFA, including two-factor authentication (2FA), relies on a minimum of two separate authentication factors to verify a user. The first factor is typically a password. The second (and possibly third) factor could be a thing you know, like a PIN or security question; a thing you have, like a device, one-time code/password, or hardware/software token; or a thing you are, including biometrics like fingerprint and Face ID, or contextual signals like location.

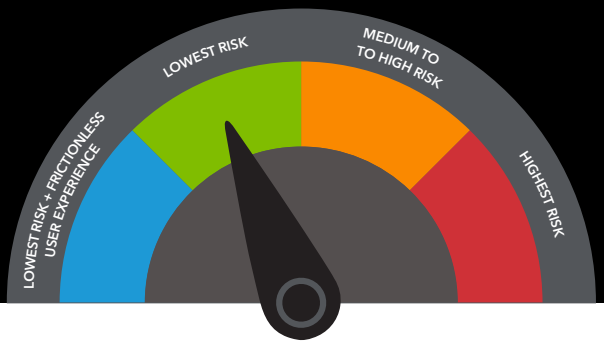
While traditional MFA greatly reduces risk in comparison with single-factor username/password authentication, it is still vulnerable to multiple methods of bypassing authentication security:

- **Phishing**
- **Use of transparent proxies (man-in-the-middle [MITM] attacks)**
- **Authentication code interception via email or SMS**
- **Credential stuffing**
- **Replay attacks**
- **SIM swapping**
- **Social engineering**
- **Vulnerabilities in online pages handling MFA operations**

There are many well-documented examples of threat actors bypassing multi-factor authentication. One such high-profile breach in 2020 was accomplished using a combination of social engineering and phishing to bypass an MFA solution, and could have been prevented with the use of physical security keys.

Lowest Risk

FIDO2 MFA via physical security key



FIDO2 is the strongest standards-based authentication method available and solves for the security vulnerabilities of traditional MFA, eliminating the risks of phishing, MITM, and replay attacks. The FIDO2 standard consists of the World Wide Web Consortium's Web Authentication specification and the FIDO Alliance's corresponding Client to Authenticator Protocol. This authentication model enables the future of MFA – authentication via cryptographic login credentials that never leave the user's device and are never stored on a server. FIDO2 also supports the eventual evolution to fully passwordless authentication.

The downside is that the only way to enable FIDO2 MFA is to purchase physical security keys for every user to use as an authentication factor.

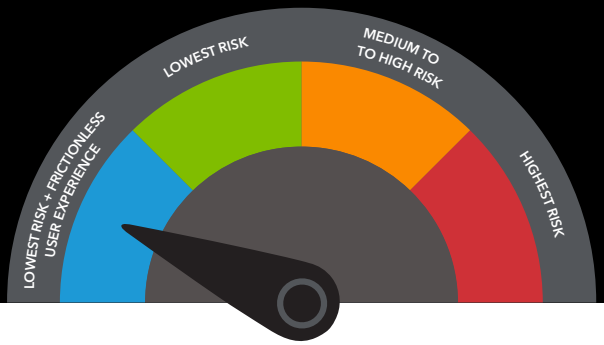
While FIDO2 is the most secure standard, implementation via hardware security keys can present many challenges:

- **Cost of buying and maintaining keys for each user**
- **Complexity of distribution and management of keys**
- **Replacing lost hardware keys**
- **Inability to update or patch hardware keys**
- **Uneven distribution – only certain employees get keys**

Purchasing, configuring, issuing, and managing physical hardware keys for all employees is costly and time-consuming. Additionally, requiring users to plug a physical key into their device for every login decreases productivity by adding a cumbersome user experience.

Lowest Risk + Frictionless User Experience

Next-Generation MFA at the Edge



Akamai MFA is a next-generation FIDO2 solution that features a phish-proof authentication factor, secured by cryptography. The service leverages a smartphone application in place of a physical security key, solving the challenges that frequently prevent enterprises from implementing FIDO2 MFA. It can be quickly and easily deployed using an existing smartphone, providing the highest level of authentication security with a frictionless user experience. Akamai MFA eliminates the risk of phishing and supports the eventual evolution to the passwordless future of authentication.

Learn more about Akamai MFA and start a free 60-day trial here: **akamai.com/mfa**.

Sources:

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 03/21.