SOLUTION BRIEF

AXIAD

Future-Proofing Your MFA

The MFA Myth: Why Over 70% of Enterprise Breaches Still Involve Compromised Credentials despite MFA

Organizations widely believe that multifactor authentication (MFA) is sufficient to protect employee credentials from cyber threats, but the reality tells a different story. Over 70% of enterprise breaches involve compromised identity credentials, proving that not all MFA is created equal.

Attackers are evolving faster than traditional MFA methods can keep up. MFA fatigue, push bombing, SIM swapping, OTP interception, and man-in-the-middle attacks have shown that weak MFA implementations are no longer viable. Without phishing-resistant MFA, organizations remain vulnerable despite having multiple authentication layers.

How MFA Became "Barely Good Enough"

MFA was initially designed to enhance security by requiring multiple authentication factors. However, widespread attacks show that MFA security varies greatly depending on how it is implemented. Traditional MFA methods such as SMS, push notifications, and one time passwords (OTPs)—are no longer sufficient because:

- Phishable MFA – SMS codes, push approvals, and OTPs can be
- MFA Fatigue Attacks – Attackers repeatedly send MFA prompts until users approve access out of frustration.
- Man-in-the-Middle (MiTM) Attacks – Tools like Evilginx bypass MFA by stealing session cookies.
- SIM Swapping & OTP Interception – Attackers exploit telecom vulnerabilities to redirect authentication messages.

Phishing-Resistant MFA: The Future of Secure Authentication

To future-proof authentication, organizations must replace vulnerable MFA methods with phishing-resistant alternatives like FIDO2 and PKI-based authentication. These methods eliminate the reliance on passwords, OTPs, and push notifications—removing the attack vectors exploited in modern breaches.

- Passwordless Authentication - Eliminates passwords and shared secrets that attackers can steal.
- FIDO2/WebAuthn – Uses cryptographic authentication with device-bound passkeys for strong security.
- PKI-Based Authentication – Ensures identity verification with digital certificates for secure enterprise access.
- Device Trust Enforcement – Only allows authentication from registered and secured devices.

HOW ORGANIZATIONS CAN FUTURE-PROOF THEIR MFA STRATEGY

PKI Strengthens and Extends MFA

Public Key Infrastructure (PKI) enhances MFA security by enabling cryptographically sound authentication through digital certificates, which makes it ideal for enterprise use cases. FIDO solutions are similar, but not the same. FIDO passkeys were designed for end user access to web sites and retain a very "consumer centric" flavor for that reason. They are not, however, well suited to all the other activities that take place daily in the commercial or business environment, like securing machine-to-machine connections, digitally signing and encrypting emails or signing documents. For this reason, the ideal MFA solution would support both PKI-based and FIDO-based credentials. Key benefits include:

- Certificate-based authentication ensures identity verification without passwords.
- Integration with FIDO2/WebAuthn provides strong, phishing-resistant authentication.
- Secure machine-to-machine communications using X.509 certificates, TLS, and SSH.
- Meets security compliance standards such as NIST 800-63 or FedRAMP.

Organizations that fail to adopt future-proof MFA are not just at risk of breaches—they are also falling behind regulatory compliance and may face penalties for weak security practices.

Double Down: Adding PKI and FIDO to Existing MFA

Organizations should ask themselves: "How do we manage these credentials, at scale, and how do we use them effectively within our MFA workflows?" To move beyond legacy MFA and transition to a scalable, phishing-resistant, future-proof MFA authentication model, organizations should deploy a credential management system supporting these three principles:

- Consolidation – Serve all MFA needs, including hardware security keys, PKI, and FIDO passkeys, in a unified system.
- Consistency – Ensure a seamless authentication experience across devices, applications, operating systems, and cloud environments.
- Cryptographically sound – System must be architected for best-practices security, including isolation by the customer, encrypted communications, and key storage in specialized hardware.

MFA is no longer a security guarantee—it is a target for attackers who exploit its weaknesses. Organizations must upgrade to phishing-resistant MFA by leveraging FIDO2, PKI, and device-bound authentication methods. Future-proofing authentication is no longer optional—it is a necessity for securing identity credentials against modern cyber threats.

To read more about how Axiad products can help your MFA evolve without ripping and replacing existing systems, visit us at axiad.com.

101 Metro Drive, Suite 560 San Jose, CA 95110 United States

AXIAD