



Delinea



Best Practices for Verifying Privileged Users with MFA at depth

High-profile breaches make headlines weekly. Most involve the use of compromised privileged credentials. Yet, only a small percentage of cyber risk and security professionals believe that username and password-based security is an adequate form of protection. As such, many organizations are turning to Multi-factor authentication (MFA) to validate the user, one of the core requirements for achieving a best practice, least privilege posture. By requiring a second authentication factor, you can block cyberattackers from accessing critical systems and network devices.

Cyberattacks not only result in data theft, but also in negative impact to the public image of the affected companies. Largely because of this, security has become a C-suite and boardroom-level discussion. No one wants to be the next headline.

To combine protecting systems and data, organizations need to deploy security that goes beyond relying on network-based perimeter defenses. Today, hackers rarely are hacking in. They're logging in. They exploit legitimate privileged user credentials to walk through the proverbial front door. As a result, in today's hybrid IT environment, leading organizations are securing the new perimeter – administrative privileged access credentials.

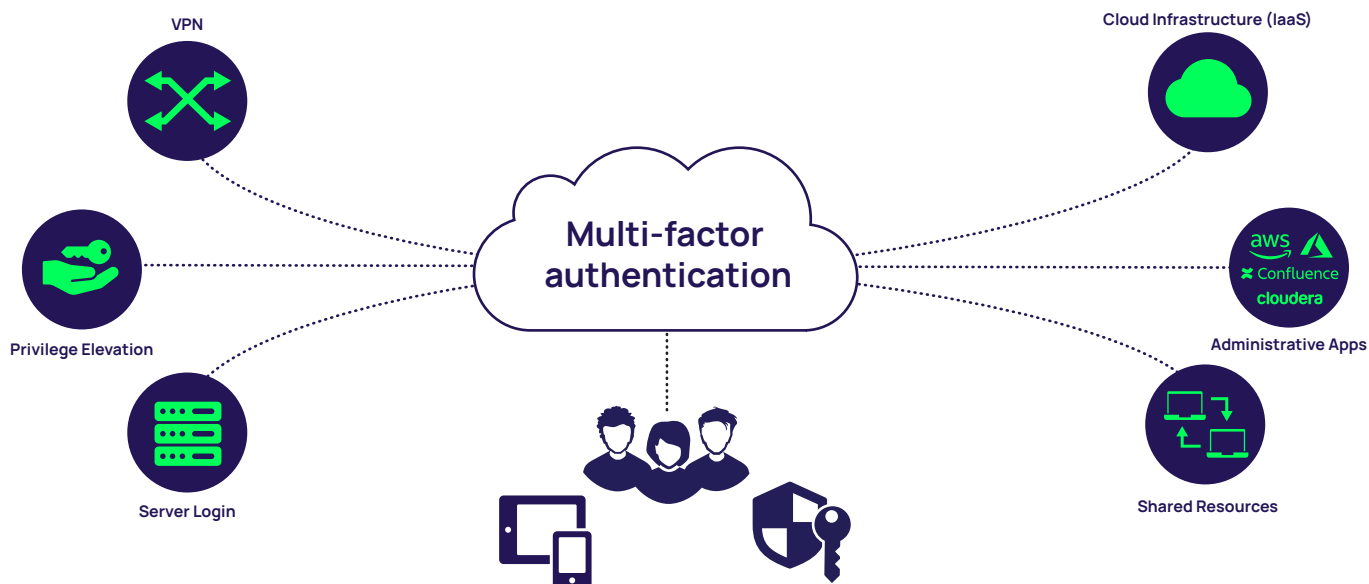
MFA mitigates access-related risk by requiring additional factors of authentication.

Implement MFA across the enterprise

Historically, organizations attempting MFA to secure all administrative access touchpoints, have failed due to incompatible and inconsistent IT administration and overhead, and user complaints.

Deploying MFA piecemeal, in silos, leaves companies exposed to attack. Security teams need to implement seamless MFA consistently for all the critical system access points within the organization. This includes both on-premises and cloud-hosted resources.

Figure 1:



Cloud transformation projects are resulting in organizations of every shape and size moving data and workloads to the cloud. Many mistakenly believe the cloud requires a separate PAM infrastructure to on-premise. This is not the case. They can implement PAM consistently across the hybrid IT infrastructure, to ensure blanket coverage, a consistent policy model, and compatible controls. This includes MFA for a growing remote workforce – internal IT as well as third-party and outsourced contractors – to reduce the risk of a breach during remote access to the internal network, login to IT systems and

network devices, as well as during privileged command or application execution.

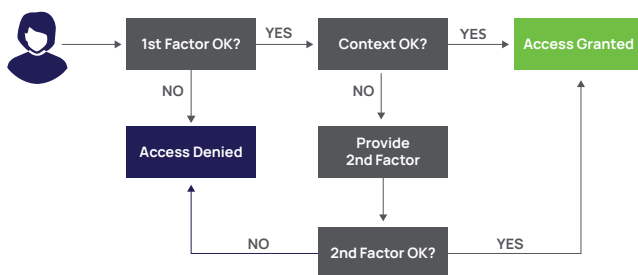
These access control points are common links in the cyber-attack chain that must be secured with MFA. Just because a legitimate ID and password was presented, does not guarantee the user at the keyboard is not an attacker (or even a bot or malware). Many publicized breaches involve legitimate credentials being obtained through various means such as phishing or Dark Web purchases, resulting in breaches that could have been averted with the use of MFA.

Leverage contextual and adaptive MFA

Rather than an “always-on” approach to MFA, organizations should use an adaptive or step-up approach to provide users with a better experience, only exposing them to MFA when necessary.

Step-up authentication, as depicted in Figure 2, is based on static rules such as time of day, location, and whether the user’s device is known. If the user’s context doesn’t match the rules, the authentication process can trigger MFA, prompting the user for a second factor to better assure identity.

Figure 2:



Adaptive authentication, also known as risk-based authentication, is like step-up authentication, but it is dynamic instead of static.

It automatically creates a user behavior profile over time and compares user activity with that baseline to determine a risk score. If the risk score is too high, the authentication process can also trigger MFA.

A key benefit of these approaches is the improved user experience. Rather than constantly being asked for MFA, the user is asked to provide an additional factor only when necessary. For example, a user logging in from the corporate network on a managed device might be granted access with a single factor, a password. However, a user logging in from an unknown network on an unmanaged device might be asked for extra authentication.

User experience is critical for successful MFA. Organizations need to balance user convenience and security. A “one-size-fits-all” approach for authentication factors doesn’t provide flexibility to implement an MFA solution that suits different user populations.

Figure 3: Incorporating a wide range of authentication methods gives users flexibility and choice, improving the user experience.



There are a wide range of authentication methods available including:

- **Hardware Tokens:** These are small hardware devices that a user carries to authorize access. They come in different forms, including smart cards, key fobs, and USB devices. The hardware device generates a one-time password (OTP) that the user enters when prompted.
- **Single-Factor Cryptographic Devices:** FIDO U2F and its passwordless successor, FIDO2, are authentication standards driven by the FIDO Alliance. They are designed to be open, secure, private, and easy to use. Hailed as the next generation Two-Factor Authentication, FIDO U2F and FIDO2 include heightened security, as public key cryptography protects against phishing, session hijacking, and malware attacks, as well as ease of use and high privacy.
- **Soft Tokens:** These are software-based tokens or applications that generate a one-time password (OTP). They are typically mobile apps installed on a smartphone and can take advantage of push notifications for improved user convenience. The widespread adoption of mobile devices has made soft tokens a popular option. Soft tokens have two main advantages over hardware tokens.

First, users are less likely to lose or forget their phones than a single purpose hardware token. Second, soft tokens are easier and less expensive to distribute to users.
- **SMS/Text message:** An OTP can be sent to a phone via SMS. Once received, the user enters it into the login screen.
- **Phone call:** A user receives a phone call to a registered phone number (landline or mobile number). The user then provides the correct response to the voice prompt to complete authentication.

- **Email:** A user receives an email with a link to verify the authentication request. Clicking on the link completes the authentication process.
- **Security questions:** Instead of tokens, users provide answers to security questions. These questions can be pre-defined or the user can define their own questions.
- **Biometric:** These methods include fingerprint, retina scans, facial recognition, and more. Many of the latest smartphones support biometrics such as Touch ID on iPhones and Fingerprint for Samsung Galaxy devices. The latest FIDO2 standard includes the ability to use on-device biometrics such as Microsoft Hello or Apple FaceID.

By offering a choice of authentication methods, users can choose which ones work best for their situation. For example, if a user's mobile phone is offline, they can still use the OTP generated via the mobile app.

Fortunately, MFA technology has evolved over the years, giving organizations the flexibility to implement an MFA solution that balances risk, usability, and cost.

Opt for a standards-based approach

Standards help ensure that your MFA solution can interoperate with your existing IT infrastructure. For example, an MFA solution should comply with standards such as Fast Identity Online (FIDO), Remote Authentication Dial-in User Service (RADIUS), and Open Authentication (OATH).

FIDO was described earlier. RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service. OATH is an open technology standard that enables solutions to deliver strong authentication of all users on all devices, across all networks.

Implement MFA in combination with other identity security solutions

Mitigate risk by combining MFA with other solutions such as least privilege access, which incorporates the best practices of just-enough privilege, granted just-in-time.

IT administrators who access critical resources are a common attack target to reach corporate “keys to the kingdom.” By implementing a least privilege approach – providing IT admin users with the lowest level of privilege to perform their daily duties while enabling them to elevate their privilege only when needed – you can reduce the risk associated with shared accounts.

By combining MFA with least privilege policies, you can enhance the protection of critical resources and reduce the risk associated with compromised privileged credentials.

Re-evaluate MFA on an ongoing basis

An MFA deployment is by no means a set it and forget it endeavor. Security vulnerabilities and the threat landscape are constantly changing, as are IT infrastructures, authentication mechanisms (e.g., mobile and biometrics), and the enterprise resources available to users.

Because of this dynamic environment it's important to conduct periodic assessments to make sure your MFA technology is continuing to meet the needs of users and the organization as a whole, and that it's being applied appropriately.

If the assessment turns up any issues, you'll need to make adjustments to ensure that the MFA strategy continues to deliver value.

In addition, MFA is becoming a requirement – or at least, a strong recommendation – for cyber insurance, in many regulations and standards such as PCI-DSS and NIST to protect access to systems where data resides. Be sure to continually review regulatory updates that apply to you.

Conclusion

Multi-factor authentication is an essential security control required for today's increasingly complex, hybrid IT environment, especially with new attack surfaces that include the cloud. It adds an extra layer of security for sensitive data, validating the user before granting access during login or privilege elevation, which is an essential requirement for achieving least privilege and a zero standing privileges posture.

Delinea recommends the following best practices for MFA:

- Implement MFA at every access point. Deploying MFA for only certain administrators, systems, or applications exposes you to potential attacks and exploits.
- Leverage step-up (contextual) or adaptive (risk-based) authentication with MFA that balances security and user convenience.
- Provide a choice of authentication methods for maximum flexibility and a better user experience. A variety of authentication methods helps IT address the needs of different user populations.
- Choose standards-based MFA solutions, as standards allow MFA to play nicely with your existing IT environment and helps prevent vendor lock-in.
- Combine MFA with least privilege access to further strengthen protection against compromised passwords.
- Implement granular, role-based access to cloud environments with policy-driven privilege elevation combined with session auditing and monitoring.
- Continuously re-evaluate MFA to assess whether the deployment is still meeting your needs.



See how to implement MFA at depth with centralized policy management.

[Explore the Delinea Platform](#)

Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. delinea.com

© Delinea MFAPU-WP-0324-EN