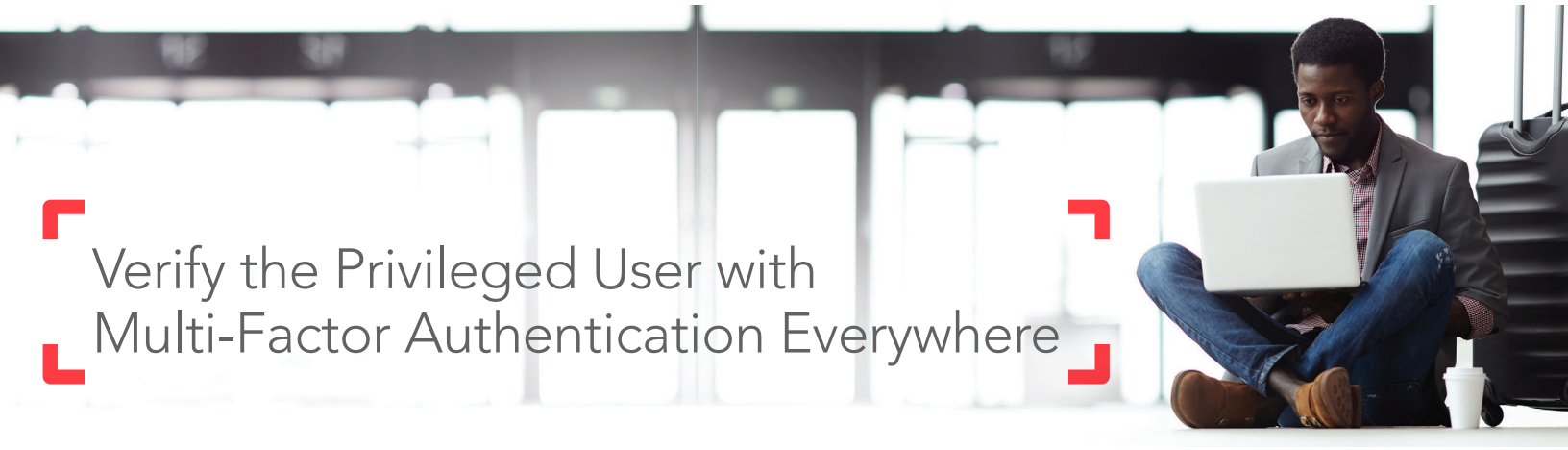


Verify the Privileged User with Multi-Factor Authentication Everywhere

High profile breaches continue to make headlines weekly. Many of these breaches involve the use of compromised privileged credentials. Only a small percentage of cyber security professionals believe that user name and password-based security remains an adequate form of protection. Many organizations are turning to multi-factor authentication (MFA) or two-factor authentication (2FA) to not only reduce the risk of stolen passwords but also to validate the user, which is one of the main concepts in helping to achieve Zero Trust Privilege. By adding a second authentication factor requirement to security policies, attackers are unable to access critical systems and network devices or gain privileged access without the smartphone (e.g., something you have) or the fingerprint (e.g., something you are) required to complete the authentication process.

Data breaches are making headlines every week. These attacks not only result in data theft, but in negative impact to the brands and public image of the affected companies. Largely because of this, security has become a C-suite and boardroom-level discussion.

Growing threats are causing companies to continuously re-evaluate their security strategy. No one wants to be the next headline. To be effective in protecting systems and data, organizations need to deploy security that goes beyond relying solely on perimeter defenses.

Most cyberthreats exploit privileged user credentials to walk through the proverbial front door. In today's hybrid IT environment, leading organizations are securing the new perimeter — user identities.

Multi-factor authentication (MFA) solutions provide the kind of protection companies need in today's increasingly complex IT and security world. MFA mitigates password risk by requiring additional factors of authentication: something the user knows, has and is.

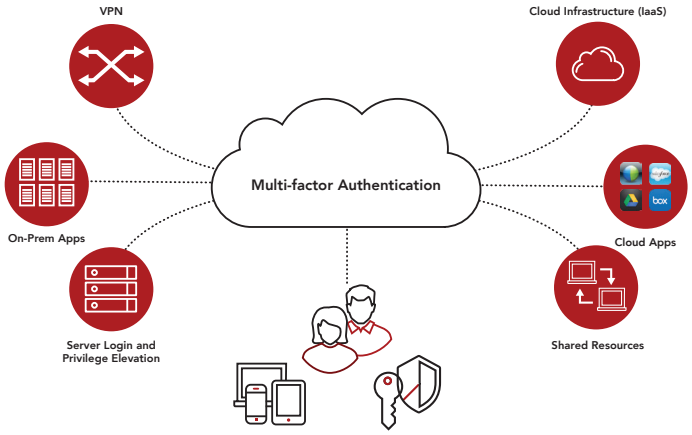
This paper examines best practices for deploying MFA.

Implement MFA Across the Enterprise

Deploying MFA in silos leaves companies exposed to attack. Security teams need to consider all the access points within the organization. This includes any cloud and on-premises resources.

More organizations are moving data and workloads to the cloud, and they need to implement consistent security across on-premises and cloud components. They also need to deploy MFA for remote network access for distributed employees and business partners.

Further, enterprises need to deploy MFA across all servers and for privileged commands. Server login and privilege elevation are common links in the cyber-attack chain. Companies, including a large financial services firm, have experienced breaches because certain servers did not have MFA.



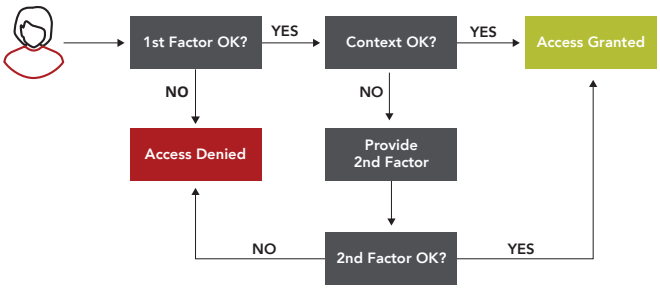
Deploying MFA everywhere, rather than in pockets or silos within the organization, enables companies to better avoid attacks. Implementing MFA across all users — end and privileged users — and across enterprise resources — cloud and on-premises applications, VPN, sever login and privilege elevation — is essential for protecting against unauthorized access, data breaches and password-based cyber-attacks.

Centrify
ZERO TRUST PRIVILEGE

Leverage Context for Adaptive MFA

Rather than an "always on" approach to MFA, organizations need to use an adaptive, step-up approach based on context. Authentication requests leverage contextual information such as location, network, device settings and time of day help determine whether the user is really who he claims to be.

As shown in Figure 2, a user authenticates with a first factor — typically a password. The authentication process also checks context (e.g. signing in from an unknown device) or behavior (e.g. accessing an application from a different location). If the context or behavior does not match the pre-defined policy, then the system triggers additional, step-up authentication.



A key benefit of adaptive MFA 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 would be granted access with a single factor, his password. However, a user logging in from an unknown network on an unmanaged device will be asked for extra authentication.

Provide a Choice of Authentication Factors

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 give companies the flexibility required to implement an MFA solution that suits the needs of different user populations.

Today, there are a wide range of authentication methods available to organizations, 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 or USB device. The hardware device generates one-time passcodes (OTP) that the user enters when prompted.
- **Single Factor Cryptographic Devices:** The FIDO U2F mechanism is an authentication standard developed by the FIDO Alliance that is designed to be open, secure, private and easy to use. Hailed as the next generation two-factor authentication, advantages of FIDO U2F include heightened security as public key cryptography protects against phishing, session hijacking, and malware attacks as well as ease of use and high privacy.

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

- **Soft tokens:** These are software-based tokens or applications that generate an 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 have 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 the user receives the OTP text message, he enters it into the login screen.
- **Phone call:** With this authentication method, a user receives a phone call to a registered phone number (land line or mobile number). The user then provides the correct response to the voice prompt to complete authentication. The advantage of a phone call (and SMS) is that the user is not required to own a modern smartphone.
- **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 and facial recognition, and more. Many of the latest smartphones support biometrics such as Touch ID on iPhones and Fingerprint for Samsung Galaxy devices.

By offering a choice of authentication methods, users can choose which ones work best for their given 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 Remote Authentication Dial-in User Service (RADIUS) and Open Authentication (OATH).

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

Companies can further mitigate password risk by combining MFA with other solutions such as least privilege access.

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 users with the lowest level of privilege to perform their daily duties while enabling them to elevate their privilege only when needed – businesses can reduce the risk associated with shared accounts.

By combining MFA with least privilege policies, organizations can enhance the protection of critical resources and reduce the risk associated with compromised 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, companies need to conduct periodic assessments to make sure their 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 assessments turn up any issues, you will need to make necessary adjustments to ensure that the MFA everywhere strategy continues to deliver value for the enterprise.

Conclusion

Multi-factor authentication is an essential security tool required for today's increasingly complex, hybrid IT environment. It strengthens securing sensitive data and helps protect user identities as well as helps validate the user before granting access to any resource, which is an essential concept in achieving Zero Trust Privilege.

Centrify recommends the following best practices for MFA:

- Implement MFA everywhere. Deploying MFA for only certain users or some applications leaves organizations exposed to potential attack and exploit.
- Leverage context for adaptive, step-up 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 other identity security solutions like least privilege access to further strengthen protection against compromised passwords.
- Continuously re-evaluate MFA to assess whether the deployment is still meeting the organization's ever-changing needs. Implement granular, role-based access to AWS with policy-driven privilege elevation combined with session auditing and monitoring.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com