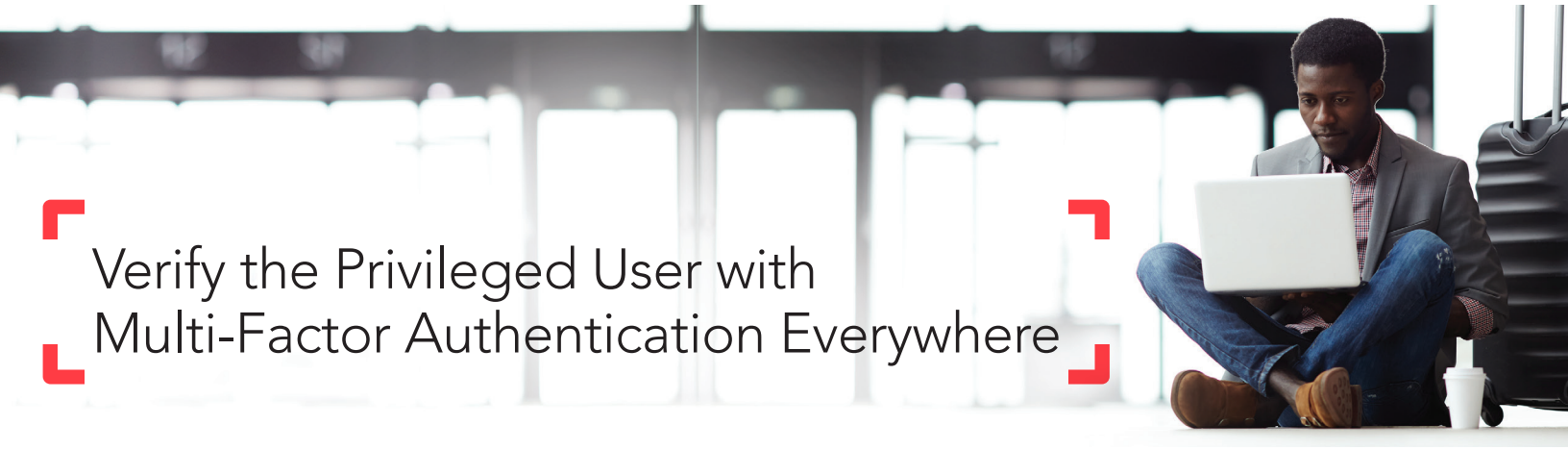


Verify the Privileged User with Multi-Factor Authentication Everywhere

High profile breaches continue to make headlines weekly. Most of these breaches 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, which is one of the main concepts in helping achieve a best practice, least privilege posture. By requiring a second authentication factor for security policies, attackers are blocked from accessing critical systems and network devices without something you have (e.g., a smartphone) or something you are (e.g., a fingerprint) to complete the authentication process.

Data breaches are making headlines every week. These attacks not only result in data theft, but also 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.

Escalating threats, combined with the cloud as a new attack surface, 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 network-based perimeter defenses.

Today, hackers rarely are hacking in. In reality 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.

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

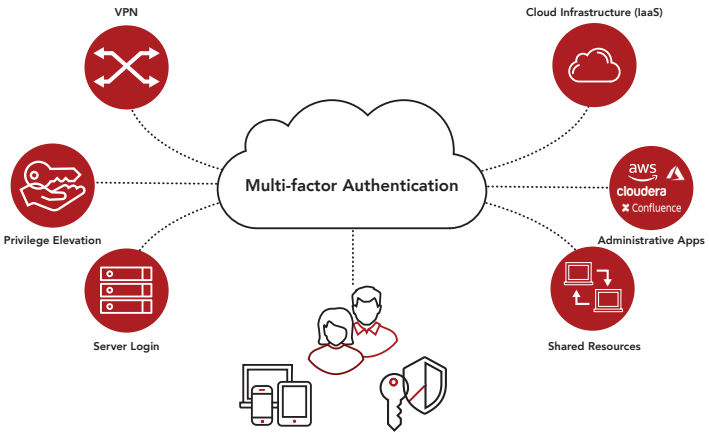
This paper examines best practices for deploying MFA.

Implement MFA Across the Enterprise

Historically, organizations attempting MFA to secure all administrative access touchpoints, have failed. Complicated MFA technologies from different vendors (incompatible and inconsistent), IT administration and help desk overheads, and user complaints about always-on MFA, have contributed to this.

Deploying MFA piecemeal, in silos, leaves companies exposed to attack. From a Privileged Access Management (PAM) perspective, security teams need to consider all the critical system access points within the organization. This includes both on-premises and cloud-hosted resources.

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 that on-premises. 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 critically 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.



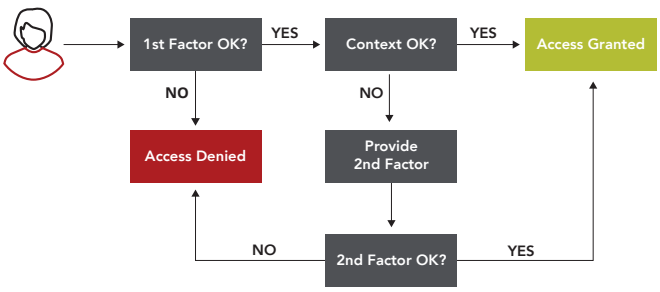
These access control points are common links in the cyber-attack chain that must be secured with MFA. Just because a legitimate ID and password was presented, is no guarantee the user at the keyboard is not an attacker (or even a bot or malware). Many publicized breaches involve legitimate credentials 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 Context for 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 current 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.

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.

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

Today, there are a wide range of authentication methods available to organizations, including:

- **Hardware Tokens:** Small hardware devices that a user carries to authorize access. They come in different forms, including smart cards, key fobs, or USB devices. The hardware device generates 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, advantages of 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:** 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.
- **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 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 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

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

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

Conclusion

Multi-factor authentication is an essential security tool 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 around your sensitive data, validating the user before granting access during login or privilege elevation, which is an essential concept in achieving least privilege and a Zero Standing Privileges posture — a best practice prescribed by Gartner.

Centrify recommends the following best practices for MFA:

- Implement MFA everywhere. Deploying MFA for only certain administrators, systems, or privileged applications leaves organizations exposed to potential attack and exploit.
- 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.
- Continuously re-evaluate MFA to assess whether the deployment is still meeting the organization's ever-changing needs. Implement granular, role-based access to cloud environments 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

www.centrify.com