Centrify
THE BREACH STOPS HERE

SOLUTION BRIEF

# Adaptive Multi-factor Authentication for Privileged Access

**Strengthen privileged access security with effective identity assurance**

**The state of computer-based breaches is reported annually by Verizon, Mandiant (a FireEye company), and other industry analysts. Each year the number of attacks grow with new vulnerabilities, exploits and tools being developed to improve the chances of breaching enterprise defenses and successful exfiltration of sensitive data. Centrify's behavior-based multi-factor authentication (MFA) for privileged access provides an extra layer of security that stops in-progress attacks on critical resources.**

## Evolving Threat Landscape = More Risk

As the number of remote administrators increases and the adoption of diverse infrastructure and applications continues, more privileged access is granted that is under less direct control.

Additional layers of security are needed to defend against human and automated attacks that target an enterprise through privileged credentials, beyond traditional perimeter and network defenses.

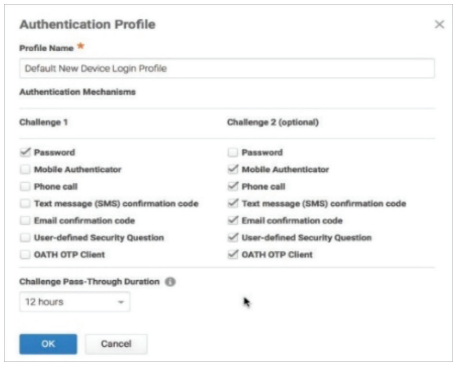
Hackers are using credentials stolen from internal administrators, third parties, and outsourced service providers to gain seemingly "legitimate" access to hybrid infrastructure.

## Multi-factor Authentication for Privileged Access

By requiring a second authentication factor in security policies, attackers are unable to misuse accounts without possessing the physical device or email address needed to complete the authentication process. This ensures the entity attempting to gain access to critical resources, whether human user or "headless", is who they say they are.

### Flexible Authentication Methods

MFA for privileged access provides flexibility to choose from a comprehensive range of second factor authentication methods. These methods include push notification to a smartphone or smart watch, soft token One Time Password (OTP) generated by the Centrify mobile app or sent via SMS/text message, interactive phone call, security questions, existing OATH-based software or hardware tokens, USB PKI keys, and Smart Cards, including derived credentials.



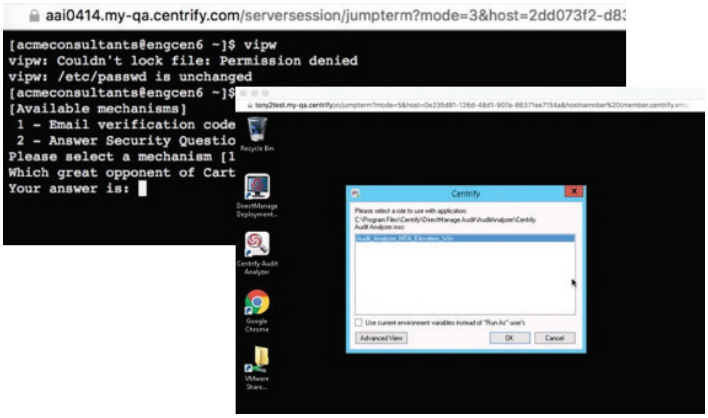

Businesses get the protection they need without sacrificing the convenience their users demand.

### MFA at Server Login

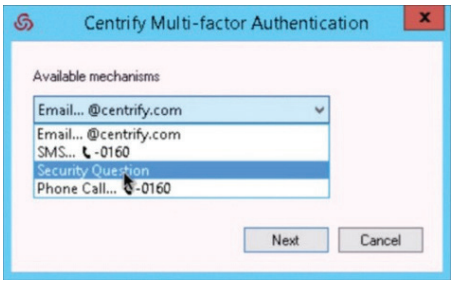
Centrify Infrastructure Services prompts for a second factor of authentication during login to Windows, Linux and UNIX servers. Building on its privileged access control capabilities, (Zones, roles, and rights), MFA is enforced on login for specific users or servers. There is no need to enforce MFA for every login event.


### MFA on Privilege Elevation

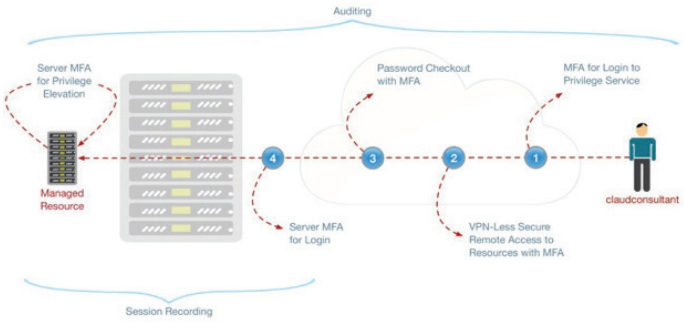
Once on the server, the user may selectively be prompted for a second factor when elevating privilege to run a highly privileged command.



## Behavior-based MFA for Session Initiation and Password Checkout




Identify anomalous behavior while it is happening by enforcing risk-aware policies for users who are initiating a privileged session or checking out a password. With a combination of risk-level and role-based access controls, user context and multi-factor authentication (MFA), IT can enable intelligent, automated, real-time decisions on whether to grant privileged access. These dynamically enforced access policies grant the user access, prompt for a second factor of authentication, or block access completely, protecting your critical resources even when users' credentials have been compromised.




MFA can also be used when checking out a vaulted password; e.g., during a "break- glass" emergency where the root account password is required for console login.

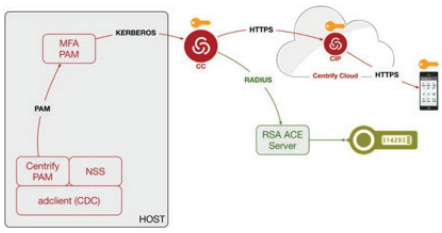
### Benefits

- Identity assurance at Windows, Linux and UNIX server login and on privilege elevation
- Strengthen zone-based authentication and authorization policies with MFA
- Protect critical resources against breach with risk-based access policies combined with MFA for session initiation and password checkouts
- Flexible MFA authentication challenges including those you already own

**RSA**

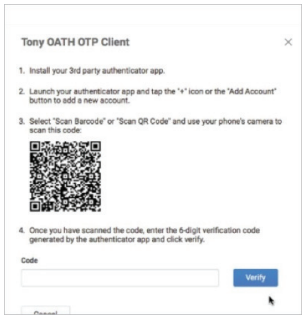
Centrify's MFA capabilities are designed to work well with existing RSA environments.

In addition to using Centrify Zones, roles, and rights to authenticate via Active Directory, the administrator can also centrally enforce RSA.




Ace/Server-based authentication and authentication policies on login to the Centrify protected server, as well as on privilege elevation on that server.

**OATH Tokens**




Investments in OATH tokens (TOTP or HOTP) such as Yubikey or Duo, can be brought under Centrify management by importing their secrets. Centrify then acts as a server to validate the OTP, and enables them to be used for portal login, remote session initiation, password checkout, server login, or privilege elevation.

**Smartcards such as PIV/CAC**

Centrify generates a cryptographic soft credential that can be stored on the card or in a secure area on a mobile device (a secure element or Trusted Execution Environment). This "derived credential" can then be used to secure access to data on desktops, laptops (Windows and Mac), tablets and mobile devices.

## MFA Everywhere You Need It

MFA for privileged access is a part of the broader Centrify MFA portfolio that extends across the enterprise. Implementing policy-based, context- aware MFA for every user (end users and privileged users), and every IT resource (cloud and on-premises apps, VPN, servers and privilege elevation) blocks cyberattacks at multiple points in the attack chain — and protects even when credentials are compromised.

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit www.centrify.com. The Breach Stops Here.




| | |
|---|---|
| SANTA CLARA, CALIFORNIA | +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 |
| EMAIL | sales@centrify.com |
| WEB | www.centrify.com |


BRF003724en-08312017