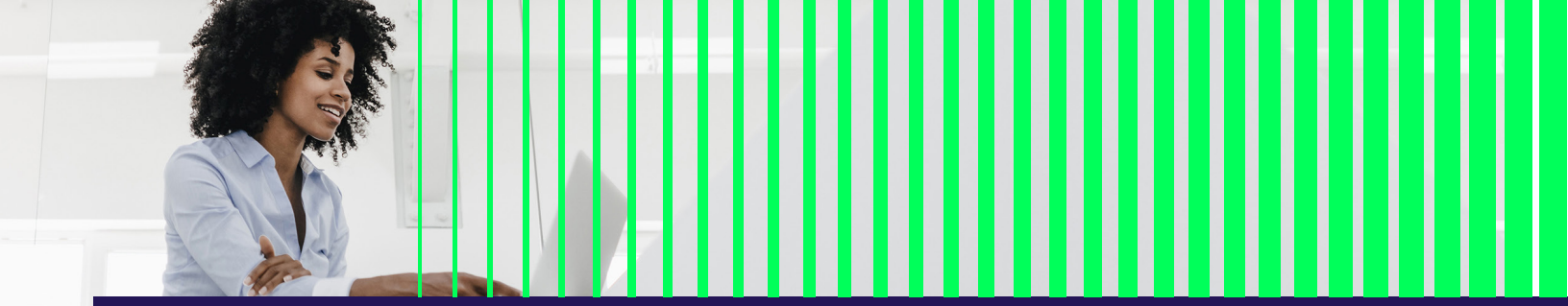


Delinea

Adaptive Multi-Factor Authentication for Privileged Access

Strengthen privileged access security with effective identity assurance

Each year the number of cyber attacks grow with hackers developing new vulnerabilities, exploits, and tools to improve their chances of breaching enterprise defenses and successfully exfiltrating sensitive data. Delinea's risk-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, organizations grant more privileged access that is under less direct control.

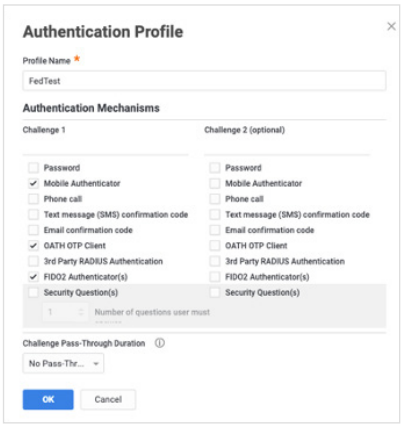
Organizations need additional layers of security beyond traditional perimeter and network defenses, to defend against human and automated attacks that use privileged credentials to target organizations.

Hackers are using credentials stolen from internal administrators, third parties, and outsourced service providers, or bought on the Dark Web, to gain seemingly "legitimate" access to IT infrastructure.

Multi-factor Authentication for privileged access

By requiring additional authentication factors 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 is a human user and is legitimate.

Flexible authentication methods



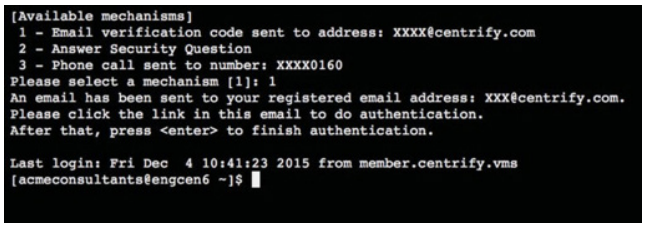
Traditionally, MFA has been cumbersome and painful for users. Authentication Profiles allow you to be selective about whether to challenge a user with one, or two additional factors, and which methods to permit. These methods include push notification to a smartphone or smart watch, soft token One Time Password (OTP) generated by the Delinea Mobile App or sent via SMS/text message, interactive phone call, security

questions, existing OATH-based software or hardware tokens, Smart Cards, and USB PKI keys including FIDO U2F and the latest FIDO2 authenticators.

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

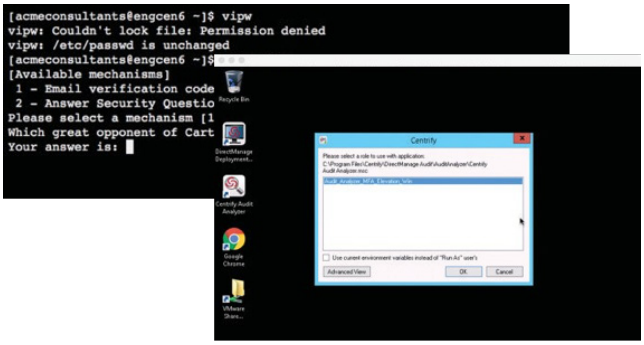
MFA at Server Login

Delinea Privileged Access Management prompts for a second factor of authentication during login to Windows, Linux, and UNIX servers. Building on its privileged access control capabilities (e.g., 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

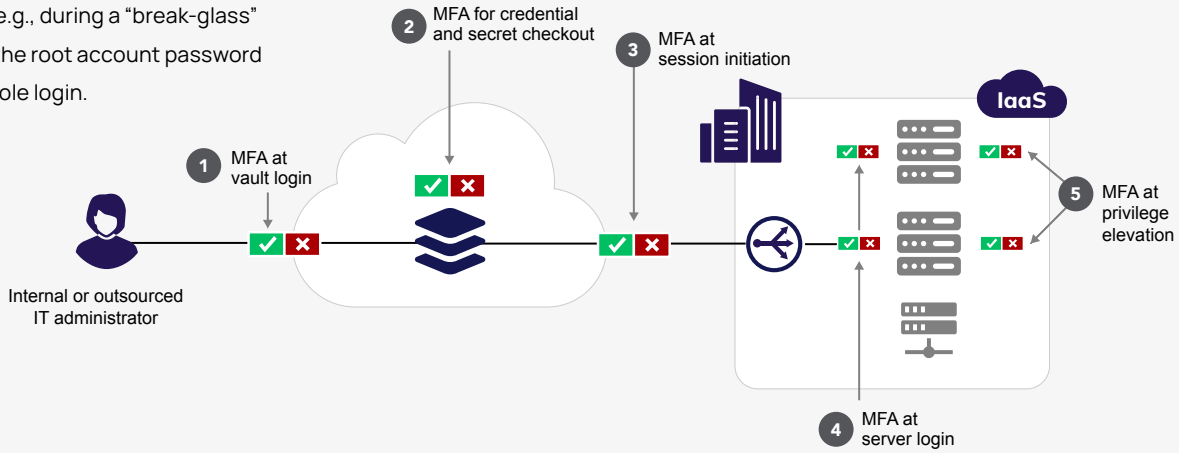
Once on the server, the user may be prompted for a second factor when elevating privilege to run a sensitive application or command. This, too, is optional.



Behavior-based MFA for session initiation and password checkout

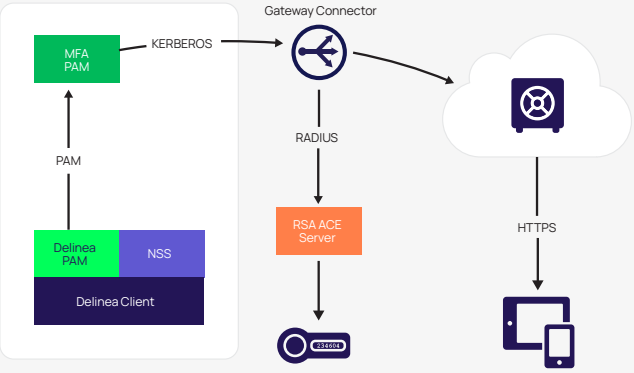
Identify anomalous behavior in real-time—not tomorrow, or next month—by enforcing risk-aware policies for users who are initiating a privileged session or checking out a password. With a combination of risk-level, role-based access controls, user context, and MFA, IT teams can enable intelligent, automated, real-time decisions on whether to grant privileged access. These dynamically enforced access policies can grant the user immediate access (i.e., no friction), prompt for a second factor, or deny 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.

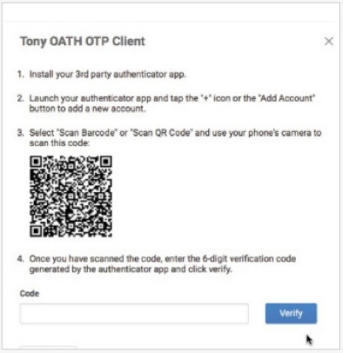


RSA

Delinea designed its MFA capabilities to work well with existing RSA environments. In addition to using our patented Zones technology, 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 Delinea protected server, as well as on privilege elevation on that server.



OATH Tokens



Bring your investments in OATH tokens (TOTP or HOTP) such as YubiKey® or Duo under Delinea management by importing their secrets. Delinea then acts as a server to validate the OTP, so you can use them at portal login, remote session initiation, password checkout, server login, or privilege elevation.

Smartcards such as PIV/CAC

While Active Directory and Windows makes it relatively easy to support smart card-based login, with Linux it's a lot harder.

Delinea makes this quick and easy. Once you have set up smart card login for Windows clients—either for a single user or multiple users—you can use Delinea to extend smart card login to Red Hat Linux clients joined to the same domain.

MFA everywhere you need it

MFA for privileged access blocks cyber-attacks at multiple points in the attack chain—and protects even when credentials are compromised.

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.

Delinea

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**