Centrify®

SOLUTION BRIEF

Multi-factor Authentication

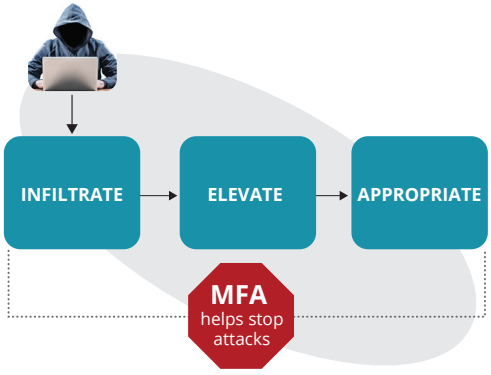
Adaptive strong authentication across your enterprise identities and resources

Passwords alone are not enough to verify a user's identity and protect businesses from data loss, fraud and malicious attacks. Login credentials are more valuable than ever, as companies adopt more cloud applications, services and infrastructure. Multi-factor Authentication (MFA) makes it harder for attackers to get in. Centrify's MFA capabilities provide additional layers of security, and helps protect organizations against the leading cause of data breaches — compromised credentials — with minimal impact to users.

Relying on simple username and password-based authentication is not enough to protect critical business data and systems against sophisticated cyber attacks. In fact, passwords are now considered security's weakest link — especially in today's cloud and mobile-enabled world.

Multi-factor authentication (also referred to as MFA) strengthens security by requiring users provide extra information or factors when they access applications, networks and servers.

Many organizations think that MFA point products alone can better secure their organization's resources and mitigate the risk of data breaches. They may implement MFA for a specific set of applications like cloud apps or for a particular group of users like employees that have VPN access. But applying MFA for only certain apps or users still leaves your organization exposed.



Attackers are relentless. They hunt, phish, spear phish, scam, and social engineer both end-users and privileged users to infiltrate your organization. Once inside they look for opportunities to elevate privilege and appropriate resources.

Implementing adaptive MFA across every enterprise user (end and privileged users, internal and external) and resource (cloud and on-premises apps, VPN, servers and privilege elevation) can thwart attackers at multiple points in the attack chain. By limiting the usefulness of any compromised credentials that attackers may have acquired or created, MFA restricts their ability to move laterally within the organization.

Centrify helps enterprises bolster security against attacks based on compromised credentials with adaptive MFA across enterprise identities and resources. Built into the Centrify Identity Platform, Centrify's adaptive MFA capabilities give organizations the ability to easily combine simple, strong authentication with single sign-on (SSO) and privileged access security.

Centrify's adaptive MFA features include customized policies for adaptive access, a broad choice of authentication factors, and a user-friendly experience.

Adaptive Authentication

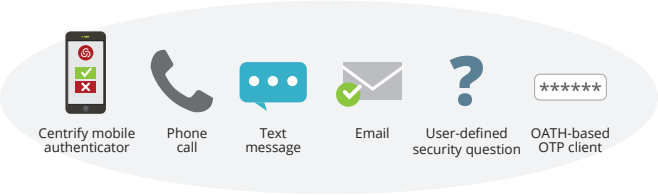
Stronger security is good, but not if it gets in your users' way. Traditional MFA is either "on" or "off", which results in constant prompting for an additional factor and annoyed users. Organizations need stronger and smarter security based on context.

Centrify Identity Platform's™ adaptive, step-up authentication delivers convenient, hassle-free strong authentication. It allows organizations to progressively challenge for MFA with flexible, context-based policies. Employees can easily and securely access applications and resources as long as they meet pre-defined policy rules. If a user does not comply with the access rules in place, they will be prompted for an additional authentication factor before access is granted. Define when to challenge for MFA based on location, device details, network, time of day, user attributes and more.

Flexible Authentication Methods

Organizations require a choice of authentication methods to make MFA as painless and easy as possible to use.

The Centrify Identity Platform provides flexibility to choose from a comprehensive range of authentication methods. Choose from push notification to a smartphone or smart watch, soft token 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. Enterprise get the protection they need without sacrificing the convenience their users demand.



MFA Use Cases

Secure Application Access

Employees demand anytime, anywhere access to applications in the cloud, on mobile devices, and on-premises. As the number of applications grow, so do the number of passwords. These passwords are often weak, re-used across apps, and shared among employees. This password sprawl increases risk, and makes strong authentication critical to protecting against data breaches and unauthorized access.

Centrify Identity Service™ helps mitigate password risk. It simplifies and secures access to applications with adaptive MFA integrated with SSO using federation standards like SAML and OpenID Connect.

Secure VPN Access

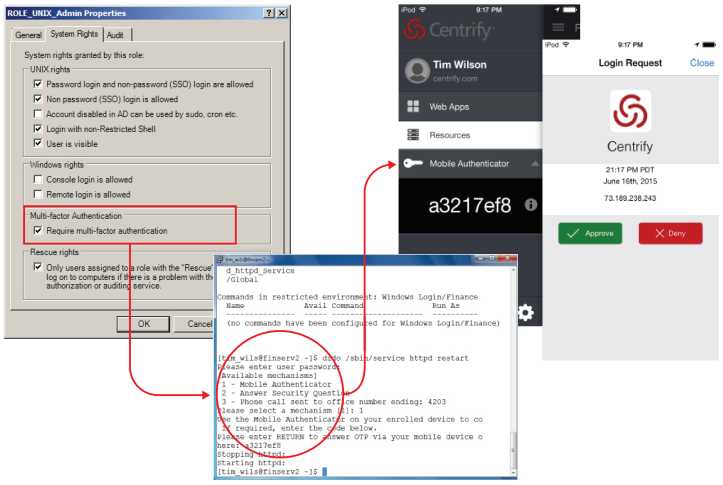
Today's mobile and remote workforce needs secure access into their organization's systems, applications and networks. VPNs are one way companies provide that access,
by establishing an encrypted connection, or "tunnel" between a remote endpoint and the internal network. But any external connection that is permitted to access resources behind the firewall poses a significant security risk. A number of high profile data breaches started with attackers compromising VPN credentials, allowing them access to an organization's internal systems.

Identity Service reduces VPN risk with MFA for any VPN that supports RADIUS. A majority of enterprise-class VPNs support RADIUS to manage remote user authentication, including Cisco, Juniper Networks and Palo Alto Networks. Adding MFA to VPN access allows organizations to give employees and partners secure remote access to their corporate network, on-premises applications and resources.

To further reduce remote access risk, Identity Service optionally provides secure, per-app, encrypted connections via On Premises App Gateway. When combined with MFA, users get simple, secure access to specific on-premises apps, without full network access.

Secure Privileged Access

Internal and outsourced IT administrators who access critical resources such as servers and network devices are a common attack point to reach corporate "keys to the kingdom." By adding a second authentication factor requirement to security policies, attackers are unable to gain privileged access without possessing the physical device or email address needed to complete the authentication process.



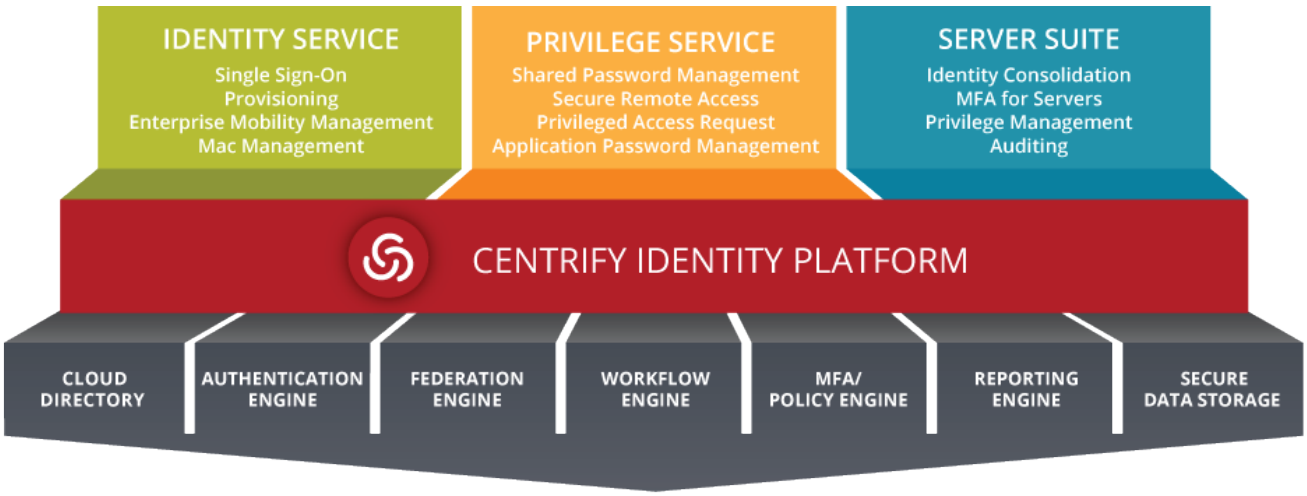
Authenticating to any system resource in the datacenter or in Infrastructure-as-a-Service (IaaS) can also be strengthened with MFA. Centrify Server Suite® provides role-based MFA utilizing its unique zone-based policies, and leverages the Centrify Identity Platform for step-up authentication services. Servers communicate securely with the on-premises Cloud Connector to request multi-factor authentication process via Centrify Identity Platform.

Benefits of Centrify Multi-factor Authentication

- Bolster security for every enterprise user — end and privileged users, internal and external
- Protect a broad range of enterprise resources – cloud and on-premises apps, VPNs, servers, privilege elevation and more
- Make MFA easy for your users — balance convenience, security and cost with adaptive MFA
- Reduce cost and complexity with an integrated identity platform
- Eliminate security gaps with one consistent set of authentication policies
- Strengthen security with the combination of MFA, SSO, least privilege access policy, and more

Centrify Identity Platform

The Centrify Identity Platform is a next-generation enterprise identity platform purpose-built to protect both end-user and privileged user identities. It unifies identity to minimize the attack surface, control access and gain visibility across today's hybrid IT world of cloud, mobile and data center. A single, integrated Identity Platform also enables enterprises to avoid the higher costs and potential security gaps associated with procuring, integrating and deploying disparate identity solutions designed for just one silo of users or resources. Centrify's identity products — Identity Service, Privilege Service™ and Server Suite — are built on top of the Centrify Identity Platform, allowing enterprises to take advantage of a number of shared identity services, including adaptive MFA.



Centrify

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. www.centrify.com.

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