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 passwords for authentication is not enough to protect critical applications, endpoints and infrastructure that house sensitive business data. 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 to provide extra information or factors unique to what the user knows, is or has.

Many organizations think that standalone MFA products can better secure their organization's resources and mitigate the risk of data breaches. They may implement MFA for a specific set of applications 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 (internal, privileged, external) and resource (applications, endpoints, infrastructure) 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. Centrify's adaptive MFA capabilities enable organizations with the ability to enforce strong authentication with a broad choice of authentication factors.

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, smarter and risk aware security controls to identify and take action on risky authentication activity.

With Centrify's analytics and machine learning engine, access control policies to applications, endpoints and infrastructure can be configured to allow SSO access to a resource, challenge the user with MFA or block access entirely. Define when to challenge users with MFA based on pre-defined conditions such as location, device, day of week, time of day and even risky user behavior.

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 mobile device; a soft OTP token generated by the Centrify mobile app, SMS/text message or email; interactive phone call, security questions, existing OATH-based software or hardware tokens, FIDO U2F security keys, and Smart Cards, including derived credentials. Enterprise get the protection they need without sacrificing the convenience their users demand.
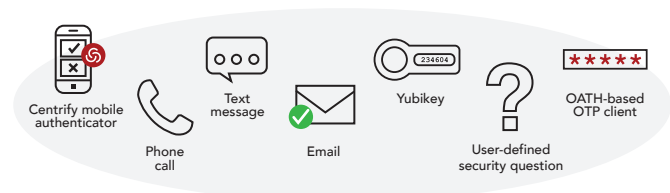
MFA Use Cases

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 Application Service™ helps mitigate password risk. It simplifies and secures access to applications with adaptive MFA and conditional access controls integrated with SSO using federation standards like SAML.

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.

Centrify reduces VPN risk with MFA enforcement on any VPN client that supports RADIUS, which include Cisco, Juniper Networks and Palo Alto Networks. Enforcing MFA for 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, Centrify provides secure, per-app, encrypted connections via an 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 server infrastructure in the datacenter or on Infrastructure-as-a-Service (IaaS) cloud platforms can also be strengthened with MFA. Centrify Infrastructure Services provides privilege access management with powerful adaptive MFA and

policy driven access leveraging the Centrify Identity Platform. Servers communicate securely with an on-premises connector to initiate a multi-factor authentication challenge/response process via Centrify Identity Platform.

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 — Application Services, Endpoint Services and Infrastructure Services — are built on top of the Centrify Identity Platform, allowing enterprises to take advantage of a number of shared identity services, including adaptive MFA and policy driven access controls.

Benefits of Centrify Multi-factor Authentication

- Bolster security for all users — internal, external, privileged, contractors and business partners

- Protect a broad range of enterprise resources – cloud and on-premises apps, workstations, network devices, servers and more

- Choose from a variety of authentication factors based on compliance requirements such as NIST

- Make MFA easy for your users — balance security and productivity with adaptive and risk aware MFA

- Reduce cost and complexity with an integrated identity platform

- Eliminate security gaps with one consistent set of authentication policies for users and resources

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 — Application Services, Endpoint Services and Infrastructure Services — are built on top of the Centrify Identity Platform, allowing enterprises to take advantage of a number of shared identity services, including adaptive MFA and policy driven access controls.

ANALYTICS SERVICES

Risk-based User Scoring   ›   Behavior Analysis and Reporting

Application Services	Endpoint Services	Infrastructure Services
Single Sign-on	Device Management	Identity Broker
Adaptive MFA for App Access	Adaptive MFA for Endpoints	Adaptive MFA for Privileged Access
Workflow & Lifecycle Management	App Management	Privilege Elevation
Mobility Management	Endpoint Privilege Management	Shared Password Management
App Gateway	Smartcard & Derived Credentials	Privileged Access Request
		Secure Remote Access
		Auditing & Monitoring

IDENTITY SERVICES PLATFORM

Directory   ›   Policy   ›   Federation   ›   Workflow   ›   Reporting

---