CENTRIFY AUTHENTICATION SERVICE

Consolidate Identities to Reduce the Attack Surface

Today's threatscape differs dramatically from the past, where humans accessed an organization's infrastructure, databases, and network devices which all resided inside a well-defined boundary. Nowadays, privileged access management (PAM) must handle requesters that are not only human but also machines, services, and APIs. There will still be shared accounts, but for increased assurance, best practices now recommend individual identities, not shared accounts, where least privilege can be applied. Whether working to mitigate the risk of insider threats or to meet PCI DSS, SOX, or other industry mandates and government regulations in an increasingly heterogenous and distributed environment, IT organizations require an Identity-Centric Privileged Access Management solution that enables centralized visibility and control over identities, privileged access management, and privileged user activity.

Legacy PAM is Not Enough for Today's Threatscape

Legacy PAM has been around for decades and was designed back in the day when all privileged access was constrained to systems and resources inside an organization's network. At any time and for as long as they wanted, sysadmins would check out a shared "root" account from a password vault, to log into a server, a database, or network device. Legacy PAM served its purpose.

However, not only is today's environment different, but cyber adversaries are taking advantage of compromised privileged credentials when executing their attacks. Organizations, therefore, must eliminate local and shared privileged accounts and their static credentials and instead use unique, individual accounts along with temporary access tokens to reduce their attack surface and ultimately strengthen their security posture. In turn, many industry and regulatory standards like NIST 800-63 and PCI DSS are beginning to mandate security controls that call for higher assurance levels than vaults can provide.

Going Beyond Discovering and Vaulting Passwords

The Centrify Authentication Service provides customers with the needed capabilities to go beyond the vault and allows properly verifying who requests privileged access. This is achieved by leveraging enterprise directory identities, eliminating local accounts, and decreasing the overall number of accounts and passwords, therefore reducing the attack surface.

> "We needed to get away from admins having to use multiple IDs — or worse — sharing a common identity on the same box...Centrify has allowed us to accomplish all of our goals."
>
> **SCOTT TEIPE, MANAGER OF INFORMATION SECURITY FOR GOGO, INC.**

MULTI-DIRECTORY BROKERING

Simplify user authentication to servers and network devices from any directory service including Active Directory, LDAP, and cloud directories. Organizations can stand up infrastructure in the cloud avoiding new siloed identity repositories, directory replication, or complex synchronization mechanisms.

ACTIVE DIRECTORY BRIDGING

Secure Linux and UNIX with the same identity services used to secure access to Windows systems. Centralize cross-platform policy management, enabling user login to any system via a single Active Directory account. Provide deep Active Directory integration for even the most complex multi-forest architectures.

GROUP POLICY MANAGEMENT

Manage authentication, access control, and group policy for non-Windows systems the same as Windows. Use Active Directory group policy to automate firewall and SSH configuration, decide which users can connect to each system, drop inactive sessions, and act as a network-based authentication.

CENTRIFY ZONE TECHNOLOGY

Managing local identities and privileges on each machine is complex and error prone. Centrify's patented Zone technology simplifies this by consolidating identities into Active Directory, centralizing management of users, computers, roles, and rights across Windows, Linux, and UNIX. Use hierarchical Zones to structure an RBAC governance model that's shaped to your needs.

LOCAL ACCOUNT & GROUP MANAGEMENT

For some situations, local accounts (e.g., system accounts) must exist. Centralize their lifecycle management the same way you manage native Active Directory accounts. Save time and money while increasing your IT staff's productivity.

MACHINE IDENTITY & CREDENTIAL MANAGEMENT

Enroll every machine in the Centrify Platform or Active Directory, assigning each a unique machine identity, and establishing a strong root of trust for machine-to-machine federated authentication based on a centralized trust model.

MFA AT SYSTEM LOGIN

Login to privileged systems is often the primary attack interface, which must be protected from cyber adversaries who wish to steal information or do harm in the environment. Multi-factor authentication (MFA) at login for Linux, UNIX, and Windows servers minimizes the risk of exposure and fulfills stringent regulatory mandates like PCI DSS and NIST 800-63A. Centrify MFA can also be applied to other access control decision points for even greater risk reduction.

Simplify Cloud Transformation Projects with Multi-Directory Brokering

Cloud transformation and migration projects carry high expectations including fast time-to-production and simplification. Additional complexity and delays often result, due to IT having to extend corporate directories — such as Active Directory, LDAP, or cloud directories such as Google — to the cloud for administrative access to the hosted systems. Designed for modern use-cases, multi-directory brokering solves this. It enables system-level authentication using your in-place directories, without requiring additional identity silos, directory replication, or complex syncing, dramatically reducing costs, improving productivity, and accelerating time-to-production. Administrators can immediately log into cloud-hosted systems using their individual corporate identity, consistent with how they access on-premises systems.

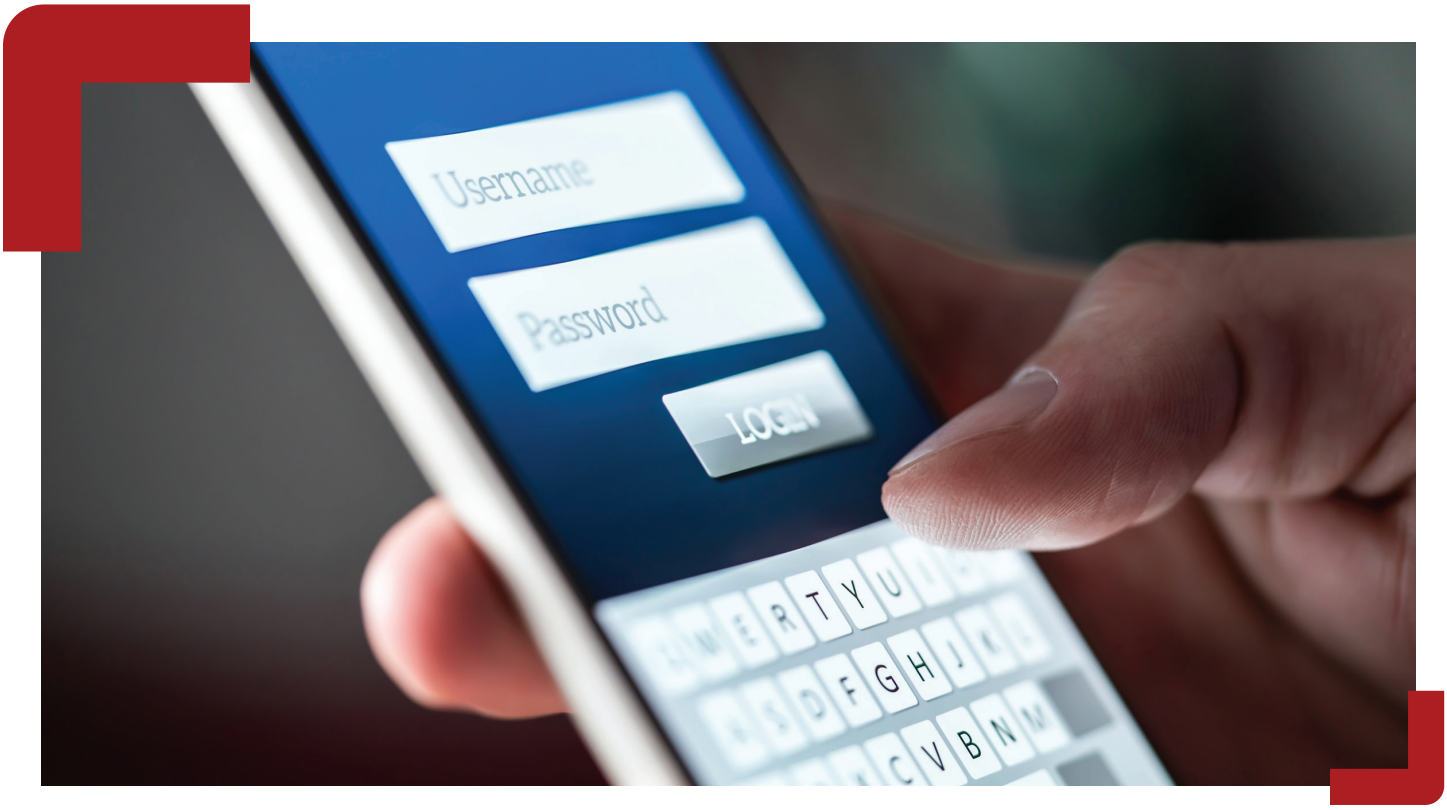
- Authenticate to privileged resources with any directory service — both on-premises and in the cloud.
- Enable centralized authentication and access controls to geographically dispersed infrastructure, leveraging identities from one or more Active Directory environments, LDAP directories, or cloud directories such as Centrify Directory or Google Directory.

Identity Management and Consolidation for Linux and UNIX with Active Directory Bridging

Centrify Authentication Service allows customers to unify their IT infrastructure by consolidating identity, authentication, and access management for Linux and UNIX within Microsoft Active Directory.

In this context, Centrify was the first vendor to integrate UNIX and Linux into Active Directory giving IT a centralized, cross-platform, management capability. Centrify us known for its unique strengths in this area, which is a popular capability among customers and prospects alike due to its tangible benefits — increased IT productivity, lowered IT maintenance costs, and reduced attack surface.

- Natively join Linux and UNIX systems to Active Directory, turning the host system into an Active Directory client. Secure systems using the same authentication and group policy services currently deployed for Windows systems.
- Consolidate user profiles and enforce separation of duties.
- Extend group policy management to non-Windows systems. It's the only solution to provide user and computer policies with advanced features such as group filtering and loopback



processing. Group policy configuration settings are seamlessly integrated into the Centrify UNIX Agent to manage configuration of both the system configuration and Client environment.

- While many vendors claim support for Kerberos, only Centrify provides native support for all the complexity and nuance of Active Directory.
- Time-saving automation is made easier with extensive CLI and scripting options, supporting Application-to-Application Password Management (AAPM).

Manage Local Accounts and Groups Efficiently

With the Centrify Authentication Service customers can streamline the management of local accounts and groups across their heterogenous infrastructure. Centrify automates the life cycle of local accounts and integrates with password vaults where necessary for services or applications to centralize all account and group management within one management platform.

- Centrally manage the life cycle for application and service accounts, and automatically secure credentials and access.
- Integrate local account password management with existing password vaults, automating the account registration and password vaulting for newly created accounts.
- Centralize management of local groups.

Quickly Centralize Management for Windows, Linux, and UNIX Servers

Centrify's Zone Technology enables you to manage your heterogeneous environment by tying the rights a user has on a Windows, Linux, or UNIX system with a single identity, stored, and managed in Active Directory.

- Establish hierarchy and inheritance.
- Enable rapid migration of UNIX identities into Active Directory.
- Leverage Centrify Computer Roles for unique management and security advantages.

Enforce Group Policies for Users and Heteregenous Systems

Centrify delivers comprehensive support for extending group policy management to non-Windows systems. It's the only solution to provide user and computer policies with advanced features such as group filtering and loopback processing.

- Enforce Active Directory group policies across non-Windows platforms.
- Manage authentication, access control, and group policy for non-Windows systems.

Ensure Only Authorized Humans are Accessing Your Critical Infrastructure with MFA at System Login

Login to privileged systems is often the primary attack interface which must be protected from cyber adversaries, who wish to steal information or do harm in the environment. To ensure that only authorized humans are accessing your sensitive systems, you need to enforce strong authentication through MFA. Centrify provides host- based technology, which cannot be circumvented to enforce MFA at systems login for Linux, UNIX, Windows servers, and workstations.

- Reinforce Zero Trust principles through host-based MFA enforcement on each computer that cannot be circumvented or bypassed.
- Centralized MFA service integration.
- Local MFA capabilities for UNIX and Linux.
- Windows MFA natively integrated into the login process.

Ready to Protect Against the #1 Attack Vector?

Register for a 30-day trial of Centrify's Privileged Access Management (PAM) software to minimize your attack surface and control privileged access to your hybrid environment.

Centrify enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid- and multi-cloud environments with Identity-Centric PAM based on Zero Trust principles. To learn more, visit www.centrify.com.

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