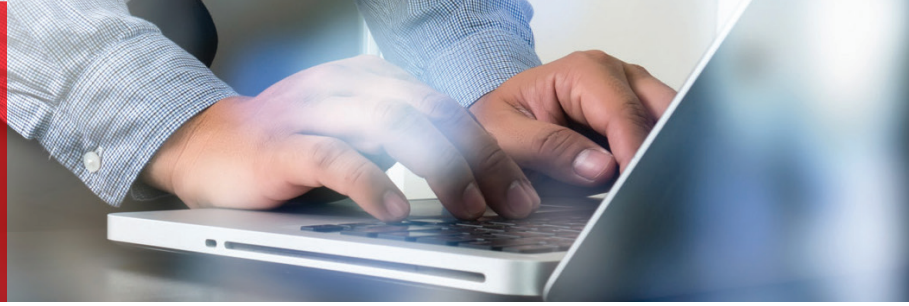
Centrify
ZERO TRUST PRIVILEGE



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 and advanced persistent threats (APTs), or to meet PCI DSS, SOX, or other industry mandates and government regulations in an increasingly heterogenous and distributed environment, IT organizations require a cloud-ready Zero Trust Privilege 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. The environment was systems admins with a shared "root" account that they would check out of a password vault, typically to access 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 accounts with static credentials on systems and instead use federated, individual accounts 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 can be achieved by leveraging enterprise directory identities, eliminating local accounts, and decreasing the overall number of accounts and passwords, therefore reducing the attack surface.

MULTI-DIRECTORY BROKERING

Simplify user authentication to servers from any directory service including Active Directory, LDAP, and cloud directories. Organizations can take advantage of the benefits of the cloud without creating new siloed identity repositories or complex synchronization mechanisms.

ACTIVE DIRECTORY BRIDGING

Secure Linux and UNIX with the same identity services currently used to secure access to Windows systems. Centralize policy management and user administration for Linux and UNIX systems to enable rapid identity consolidation into Active Directory. Provides deep Active Directory integration for even the most complex Active Directory architectures.

MACHINE IDENTITY & CREDENTIAL MANAGEMENT

Centrally manage machine identities and their credentials within Active Directory or the Centrify Zero Trust Privilege Services to establish an enterprise root of trust for machine-to-machine 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. With Centrify you can beyond MFA at server login and apply MFA everywhere.

CENTRIFY ZONE TECHNOLOGY

Quickly consolidate complex and disparate UNIX and Linux user identities into Active Directory with Centrify's patented Zone technology — without having to first rationalize all user identities. Centrify Zones allows to manage users, computers, roles, and rights in a hierarchical model that you can shape to your needs.

LOCAL ACCOUNT & GROUP MANAGEMENT

Manage system accounts the same way you would managing user accounts in Active Directory. Save time and money while increasing your IT staff's productivity.

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.

Simplify Moving Workloads to the Cloud with Multi-Directory Brokering

Simplify user authentication to servers from any directory service including Active Directory, LDAP, or cloud directories such as Google's. Organizations can take advantage of the benefits of the cloud without creating new identity silos, duplicating identity repositories, or compromising the level of privileged access security and enterprise access they currently have on-premises. In addition, IT managers save time managing a heterogenous IT environment, achieving dramatic cost savings for the organization.

- 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 supporting multiple identities for a single user. In the 2018 Magic Quadrant for Privileged Access Management, Gartner specifically calls out Centrify's unique strength in this area, which is a popular capability among customers and prospects alike due to its potential to increase IT productivity, lower IT maintenance costs, and reduce the 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 user's 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.

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

Centrify
ZERO TRUST PRIVILEGE

www.centrify.com