Centrify Server Suite

Minimize Your Attack Surface and Control Privileged Access to Your On-Premises and Cloud-Hosted Infrastructure

Digital transformation is changing the enterprise landscape, creating increased complexity as organizations leverage emerging technologies such as the cloud, big data, DevOps, containers, microservices, and more. This complexity brings new challenges and requirements for identity and access management, making it essential to centralize and orchestrate these exponentially increasing and fragmented identities across a hybrid enterprise infrastructure.

Today's Modern Enterprise

IT organizations are increasingly deploying and managing hybrid environments that combine cloud-based and data center infrastructure while working to mitigate the risk of insider and cyberthreats and meet PCI DSS, SOX, FISMA, HIPPA, MAS, or other industry mandates and government regulations. Modern enterprises require a purpose-built, privileged access management (PAM) solution with a common platform that enables centralized control and visibility over privileged access and simplified compliance to protect against new and evolving identity-based threats and attack surfaces.

Privileged Identities are a Critical Focus

Underlying the foundation of digital transformation are privileged identities, meant to assure that only authorized individuals, machines, or services access the right resources at the right times and for the right reasons. But, in the wrong hands, your entire business can be at risk. Protecting them is, therefore, paramount.

Establishing a proper mechanism to do this most efficiently and securely has become the Achilles Heel, limiting many digital transformation projects' successes. The main reasons are infrastructure complexity and PAM solutions with one foot in the past, having stood still as your business needs have evolved.

You Invest in Modern Infrastructures and Application Development Tools. Shouldn't You Invest in a Modern PAM to Protect It?

Security technology of the past — including firewalls, virtual private networks (VPNs), and antivirus software — has proven to be necessary, but insufficient protection against today's data breaches. Organizations must look beyond these network-centric security solutions and to PAM to stop data breaches.

A modern PAM solution founded on Zero Trust principles takes an identity-centric approach to protect your IT infrastructure, wherever it is. Gone are the old PAM assumptions, protecting infrastructure that lives exclusively in a walled-garden datacenter.

Centrify Server Suite enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid- and multi-cloud environments. It allows humans and machines to seamlessly authenticate, enforcing least privilege with just-in-time privilege elevation, increasing accountability, and reducing administrative access risk.

©2021 Centrify Corporation. All Rights Reserved.

CENTRIFY AUTHENTICATION SERVICE

Especially in large, hybrid IT infrastructures, centralized and efficient management of users, computers, roles, and rights is critical to streamlining IT administration. Enable fine-grained access control to Windows, Linux, and UNIX systems with centralized policy management from Active Directory.

CENTRIFY PRIVILEGE ELEVATION SERVICE

Reduce the risk of a breach, and the damage administrators can do when they (or a cyber-attacker) have broad and unmanaged privilege, with a flexible, fine-grained privilege elevation service. Enforce zero standing privileges and reduce lateral movement.

CENTRIFY AUDIT AND MONITORING SERVICE

Detect suspicious user activity and alert in real-time to stop breaches in progress. Monitor and control privileged sessions that leverage shared or individual accounts, with full video and metadata capture.

Why Place Your Trust in Centrify Server Suite?

Over Centrify's history, we have developed a deep understanding of PAM, including our initial focus on centralizing and orchestrating fragmented identities across enterprise infrastructure. We were the first vendor to join UNIX and Linux systems with Active Directory and later extended similar capabilities to IaaS environments to empower cloud transformation, and offer the industry's first true multi-tenant, cloud architected PAM-as-a-Service solution (Centrify Vault Suite).

Applying our expertise in infrastructure management allowed us to evolve a more modern PAM approach and focus on identity-centric solutions based on Zero Trust principles. We believe that PAM solutions must meet the needs of both infrastructure and security teams with a single platform; they are made of the same connective tissue and therefore belong together.

Centrify Server Suite

Centrify Server Suite comprises three core products that work synergistically to fully protect your Windows, Linux, and UNIX estates against identity-based attacks. It leverages shared services delivered by the Centrify Platform, acting as a control plane.

Centrify Authentication Service

Centrify Authentication Service extends Active Directory (AD) benefits to Linux and UNIX by natively joining them to AD, turning the host system into an AD client. It secures access to these systems consistently, using the same authentication and Group Policy services currently deployed for your Windows systems. Changes to user access and permission in AD (e.g., via just-in-time access request workflow) is immediately reflected and enforced at the AD client. This overcomes inherent AD propagation delays that can disrupt time-critical activities (such as a breach investigation).

With AD for cross-platform management, you can now consolidate identities. This means eliminating the many local privileged accounts (especially on *NIX) and giving administrators a single AD account with which to access any AD-joined system, reducing your attack surface. If you must use local accounts, manage their lifecycle centrally, from AD, with Centrify Local Account and Group Management.

Manage all this complexity and chaos with Centrify roles and patented Zones technology. Zones extend the flat AD container model, so you can logically group systems in a parent-child hierarchical model that aligns with your preferred governance approach. Granting access to computers in a Zone is as simple as adding a user to that Zone.

With human user access under control, leverage this same infrastructure to better secure your DevOps environment. Leverage Centrify Vault Service to store application/service passwords and secrets. So instead of this sensitive data being exposed in code and configuration files, applications can obtain it at run-time via API or CLI calls, reducing your risk. Further, eliminate per-application service accounts required to authenticate to the vault – each of which represents a vector of attack. Leverage Centrify's unique Delegated Machine Credentials and capitalize on the machine's enrollment in the Centrify Platform and resulting mutual trust. Thus, only a single machine identity is required for access to vault services.

- AD bridging
- Brokered authentication
- Group policy for Linux
- Linux smart card login for workstations
- RBAC and Centrify Zones
- MFA at system login
- Local account and group management
- Approval workflows for login

Centrify Privilege Elevation Service

Assigning just enough privilege based on a job function increases security and accountability. Having users log in as themselves and elevate privilege based on their role within the organization minimizes your attack surface by reducing shared accounts and vaulted credentials. Instead of standing privileges, self-service workflow allows admins to request temporary roles to complete legitimate helpdesk-driven tasks for just-in-time access.

Centrify Privilege Elevation Service acts as a policy enforcement point to control privilege elevation on Windows, Linux, and UNIX systems. It consumes policy that the Centrify Authentication Service centrally defines and maintains in AD and enforces what system-level commands and applications users can execute.

- Enforce least privilege
- MFA at privilege elevation
- Approval workflows for privilege elevation
- Control privilege elevation
- Centrify Zones for RBAC policy
- Delegated Machine Credentials

©2021 Centrify Corporation. All Rights Reserved.

Centrify Audit & Monitoring Service

Gain full accountability and visibility into all privileged activity and tie everything back to the individual by recording and managing a holistic view across Windows, Linux, and UNIX servers. For PCI and SOX compliance and incident response investigations, leverage out-of-box reports.

With host-based auditing on each system, ensure that cyber-attackers can't bypass session recordings. Eliminate spoofing with advanced monitoring capabilities that combine application and file change monitoring at the shell and process levels, with video recording, metadata capture, and time-indexed command auditing. Detect attempts to spoof video recordings with commands hidden inside aliases and shell scripts.

- Host-based audit and monitoring
- Gateway-based audit and monitoring
- Linux and UNIX advanced monitoring at the shell and process levels

For data privacy, prevent visibility to sensitive data in Centrify audit logs. Centrify Audit & Monitoring Service obfuscates the data at source (i.e., on the host system) ensuring it never leaves the host system. Thus, data privacy is ensured whether events are viewed locally or forwarded to other systems (for example, Splunk).

If you need a modern PAM solution to govern and control access to on-premises and private cloud IT infrastructure, centrally managed from AD — take a closer look at Centrify Server Suite.

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 by allowing human and machine identities to seamlessly log in and granting least privilege just-in-time, increasing accountability, and reducing administrative access risk.

©2021 Centrify Corporation. All Rights Reserved.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +65 9788 2594
Brazil +55 11 3958 4876
Latin America +1 305 900 5354

sales@centrify.com

www.centrify.com