Centrify
THE BREACH STOPS HERE

Centrify Server Suite®

Unified identity management and audit across on-premises and cloud-based Windows, Linux, and UNIX Systems

Whether working to mitigate the risks of insider threats and advanced persistent threats, or to meet PCI DSS, SOX or other industry mandates and government regulations in an increasingly multi-platform and cloud- based environment, IT organizations require a unified identity management and auditing solution that enables centralized visibility and control over identities, privileged access management, and activity.

Centrify Server Suite Delivers:

IT Security & Compliance

Keep your complex, multi-platform physical and virtual data centers secure and compliant through centralized and fully integrated management of authentication, privileged access management and activity.

Identity Consolidation

Reduce risk and streamline operations by automating discovery of identity-related issues, eliminating redundant identity stores, and tying access controls and privileged accounts to a single, centrally managed Active Directory identity.

Multi-factor Authentication for Servers

Add an extra layer of security to protect against hackers by configuring multi-factor authentication (MFA) for IT administrators who access systems and require elevated privileges.

Privileged User Session Auditing

Mitigate insider threats and meet compliance requirements with full audit trails and session capture of privileged user activity on Windows, Linux and UNIX servers. Gain comprehensive visibility with unified access and activity reporting. Select or schedule packaged attestation reports or create your own.

Central Policy Control

Centrally control security and configuration policies across Linux, UNIX and Mac systems using familiar Windows Group Policy tools.

Local Account Provisioning

Centrally manage the lifecycle for application and service accounts, and automatically secure credentials and access. Minimize your attack surface by using Centrify Zones to uniformly provision and de-provision identities across the systems running your applications.

Privilege Management

Eliminate the problem of too many users having too broad and unmanaged administrative power — enable flexible, role-based assignment of privileges, enforce granular controls not possible with native Operating System tools, and tie all privileged activity to an individual.

SIEM Integration

Identify suspicious activity quickly by creating security alerts utilizing Server Suite's streamlined integration with SIEM solutions from HP ArcSight, IBM QRadar and Splunk.

Server Isolation and Encryption of Data-in-Motion

Protect sensitive Linux and UNIX servers by dynamically isolating and blocking untrusted systems from communicating with trusted systems.

KEY BENEFITS

Thwart in-progress attacks using stolen credentials on your critical systems by reinforcing secure access policies with a multi-factor authentication plan. By configuring a second authentication factor requirement, attackers are unable to misuse your accounts without possessing the physical device or email address needed to complete the authentication process.

Gain visibility into identity-related risk through automated discovery of violations of identity and access management best practices, and simplified privileged access management and auditing that links all privileged activity back to an individual (as opposed to a shared account).

Make regulatory compliance repeatable and sustainable with unified identity policies that enforce a least-privilege security model across Windows, Linux and UNIX systems and applications while also enabling enterprise-wide privileged session auditing and compliance reporting.

Reduce costs and increase productivity with a single, integrated solution for unified identity, privileged access management, and activity auditing, that leverages existing investments in identity.

Which Edition is Right for You?

EDITION	COMPONENT	PLATFORM	KEY FEATURES
Standard	DirectManage®	Windows Linux UNIX	• Automate discovery of identity and access management issues on *NIX • Rapidly migrate *NIX identities into Active Directory • Provision and manage access and roles programmatically, through scripts including Powershell, or via MMC • Advanced regulatory compliance reporting of access and activity with packaged attestation reports
	DirectControl®	Linux UNIX	• Advanced AD support (one-way trusts, zero schema mods) • Centralized identity management automates mapping of UIDs to an AD account Patented, hierarchical Zone-based management enables scale • Centrally manage the lifecycle for application and service accounts • Group Policy for Linux and UNIX • Legacy integration and migration (NIS & LDAP Proxy Servers) Centrify-enabled OpenSSH, Kerberos, PuTTY and Samba
	DirectAuthorize®	Windows Linux UNIX	• Privileged Access Management leveraging role-based authorization • Dynamic access restrictions (time, access method) • Restricted shell environment (whitelist) — UNIX • Automated implementation of least privilege access • Simple SUDO migration and replacement
Enterprise Includes Standard Edition components plus:	DirectAudit®	Windows Linux UNIX	• User session capture for Windows, Linux and UNIX User session search and replay with command list • Trigger recording based on user, role, machine or privilege elevation SQL–based event reporting and archiving
Platinum Includes Enterprise Edition components plus:	DirectSecure®	Linux UNIX	• Isolate sensitive and regulated servers dynamically • Enable end-to-end encryption of data-in-motion • PKI certificate auto issuance and renewal
All	Multi-factor authentication (MFA) for Servers[1]	Windows Linux UNIX	• Guard against cyberthreats with MFA on server login for Windows, Linux and UNIX • Stop in-progress attacks with MFA on privilege elevation for Windows, Linux and UNIX • Reinforce zone-based policies with flexible choices for MFA challenges
All	SIEM Integration	Windows Linux UNIX	• Gain visibility of in-progress attacks with security alerts created from privileged activity data

[1] Requires Server Suite plus Privilege Service

"We started out with very simple roles and now we manage user privileges with extreme granularity. The roles in Centrify are essential in limiting what people can access, and locking our systems down."

Jeff Williams
Systems Integration Chief

"With Centrify's new solution, enterprises can embrace popular Hadoop distributions with reduced identity-related risk and meet certain regulatory compliance requirements. Enterprises can leverage existing active directory security frameworks to control access, privileges, and auditing across Hadoop clusters."

FORRESTER® Critical Big Data Insight from Strata 2015, May 29, 2015

Centrify®
THE BREACH STOPS HERE™

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit **www.centrify.com**. The Breach Stops Here.

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**

DSH000045EN-041017