Centrify Privileged Access Service

Putting Core Privileged Access Controls in Place

Over the last years, it's become evident that cyber-attackers are no longer "hacking" to carry out data breaches — they are simply logging in by exploiting weak, stolen, or otherwise compromised privileged credentials. To add to this challenge, the attack surface of organizations has changed dramatically. Privileged access nowadays not only covers infrastructure, databases, and network devices, but is extended to cloud environments, Big Data, DevOps, containers, and more. Considering both internal and external identity-based threats, IT organizations must take a first step towards Zero Trust Privilege by vaulting away shared account or application passwords, as well as secrets. With the rise of mobile workforce, outsourced IT, and third-party contractors, it is also vital to secure remote access and avoid infections during remote sessions.

Privileged Accounts Hold the Keys to the Kingdom

Security breaches are all over the news. Caused by both malicious insiders as well as hackers, they are simply logging in using weak, stolen, or otherwise compromised privileged credentials. Once they are in, they then spread out and move laterally across the network, hunting for further privileged accounts and credentials that help them gain privileged access to an organization's most critical infrastructure and sensitive data.

Forrester Research has estimated that, despite continually-increasing cybersecurity budgets, 80% of security breaches involve privileged access abuse and 66% of companies have been breached an average of five or more times.

In turn, organizations need to control and monitor privileged accounts and access while improving IT productivity for both internal and outsourced IT in today's modern enterprise.

Putting Core Privileged Access Controls in Place

The Centrify Privileged Access Service allows organizations to establish the core privileged access controls across their growing attack surface. Vaulting away shared account passwords, application passwords, and secrets is just one of the best practices to secure privileged access across the modern, hybrid enterprise. Managing the vaulted credentials, leveraging secure administrative access via a distributed local jump box, establishing VPN-less privileged session to remotely access targeted infrastructure, and implementing multi-factor authentication are at the root of reducing threats, intentional or not. The Centrify Privileged Access Service grants access from a Web UI or mobile app and is available as a cloud-based service or customer-managed deployment on-premises. It covers your entire attack surface, both on-premises and in the cloud.

The service even helps organizations to increase workstations' security posture by minimizing the attack surface and controlling privileged access. Organizations can eliminate for example the use of static local admin passwords on workstations through password rotation and time-bound privileged access provided by Local Administrator Password Management (LAPM).

SHARED PASSWORD MANAGEMENT

Reduce the risk of a security breach when sharing privileged accounts, application passwords, or secrets.

CREDENTIAL MANAGEMENT

Secure, auto-rotate after check-in, and control access to passwords, SSH keys, and privileged credentials based on policy to prevent cyber-attacks and meet audit and compliance requirements.

SECURE ADMINISTRATIVE ACCESS VIA JUMP BOX

Access should only be achieved through approved Privilege Admin Consoles, which can include web-based, native client, or thick client access to sensitive systems via a locked down and clean server gateway that serves as a distributed local jump box.

SECURE REMOTE ACCESS

Provide remote admins, outsourced IT, and third-party vendors with secure access to the specific infrastructure they manage — on-premises and in the cloud. Risk-aware multi-factor authentication (MFA) combined with VPN-less access and flexible deployment models deliver the security your hybrid IT environment demands.

ACCESS REQUEST & WORKFLOW APPROVAL

Minimize your attack surface by eliminating static and long-lived privilege grants. Govern temporary access to roles that grant privilege, shared account credentials, and remote sessions with self-service access request and multi-level approvals. Capture who approved access and reconcile approved access with actual access.

MFA AT VAULT

So that we are always verifying the "who", we must apply MFA everywhere. This applies during vault login and upon password checkout, or remote session initiation…anytime there is a new request and we must know with certainty who is on the other end before granting access.

Manage Shared Accounts and Passwords Securely

While today's threatscape demands the use of individual identities rather than shared accounts to achieve increased assurance levels as mandated by newer legislation and industry best practices, there will still be shared passwords in many organizations. Thus, it's vital in a first step to discover and register all machines and then vault all shared, alternate admin, and service accounts. Access to those accounts is then brokered for users, services, and applications.

- Discover Windows, Linux, and UNIX servers, network devices, privileged accounts (local, domain, and dash-a), service accounts, and Active Directory domains.
- Secure checkout of account passwords.
- Establish sessions without disclosing passwords.
- Streamline secure privileged access for local clients.
- Apply risk-aware policies for checkouts and privileged sessions.
- Provide break-glass access to passwords from a mobile app.
- Automatically rotate on events (e.g., check-in) based on established policies or manually in mass (e.g., in response to a breach).

Secure and Manage Application Secrets

Leveraging Centrify Privileged Access Service, applications and scripts retrieve passwords and authenticate securely without human intervention, enabling organizations to meet compliance and security policies. At the same time, you can vault all your secrets — be it IP addresses, SSH keys, or others.

- Eliminate passwords from scripts and applications.
- Secure application access to privileged account credentials.
- Centrally manage secrets to reduce secrets sprawl.
- Automate management of application credentials by periodically rotating them using your enterprise-wide password policies to increase security.

Robust Credential Management Goes Beyond Vaulting and Credential Rotation

With the Centrify Privileged Access Service developers get the best of both worlds where applications can either checkout managed static credentials from a vault or leverage federation technologies for client-to-server authentication depending on which is best for the application.

- Centralized systems and service accounts.
- OAuth 2 for confidential client authentication.
- SAML tokens for Web access.

Granular Remote Access Control Without VPN

Provide your IT administration teams, outsourced IT, and third-party vendors with secure, granular access to critical infrastructure resources regardless of location and without the hassles of a virtual private network (VPN). Centrify Privileged Access Service enables secure remote access to data center and cloud-based infrastructures.

- Secure access to servers, network devices, and IaaS.
- Secure access for employees and third parties — remote and on-site — through Active Directory, LDAP, and the Centrify Directory.
- Grant access to specific resources by surgically placing the user on a specific server or network device without exposing the broader network.
- IT admins can log in and securely access resources from any location that can reach the Centrify Privileged Access Service.
- Break-glass access to passwords from a mobile app.

Eliminate The Potential for Workstation-related Infections

The Centrify Privileged Access Service provides secure, distributed jump box or bastion host capabilities to support privileged admin console activity across various private networks from a protected environment to eliminate the potential for workstation-based infections or malware from accessing sensitive systems.

- Support for privileged access to Windows, Linux, and UNIX servers either using a local RDP or SSH client, or through the built-in browser.
- Centralized access to multiple data centers, DMZ environments, or IaaS providers.
- Desktop apps support for native Windows application access (e.g., TOAD, SQL Server Management Studio, VMware vSphere).

Self-Service Privileged Access Request and Approval Workflow System

Centrify Privileged Access Service provides a built-in access request and approval workflow engine or integrations with leading IT Service Management (ITSM) software to protect your existing technology investments.

- Self-service request for privileged accounts and roles.
- Multi-level approval workflow and auditing.
- Support for mobile approval.
- Time-bound privileged access.
- Privileged access request via third party solutions (e.g., ServiceNow® and SailPoint Technologies®).

Minimize Risk, Increase Assurance with MFA at Vault

Centrify provides full MFA capabilities with the widest array of over seven choices to ensure compliance at NIST Assurance Level 2 or 3 for access to the Centrify Privileged Access Service and all protected accounts and systems.

- Native MFA support or integration with third-party MFA.
- MFA for vault login, checkout, and session initiation.

Our mission is to stop the leading cause of breaches – privileged access abuse. Centrify empowers our customers with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise attack surfaces. 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

Centrify®
ZERO TRUST PRIVILEGE