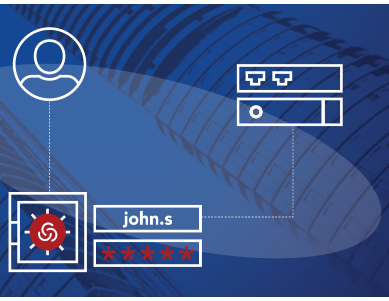
Centrify
THE BREACH STOPS HERE™

DATASHEET

Centrify Privilege Service™

Access and Password Management for the Modern Enterprise



IT organizations are increasingly required to manage hybrid deployments that combine cloud-based and data center infrastructure. IT admins, both internal and outsourced, need to login from inside and outside of the corporate perimeter. In order to meet these challenges, IT organizations that share privileged accounts need an access and password management solution built for the modern enterprise to increase security, simplify compliance and control remote access to servers and network equipment.

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 use Advanced Persistent Threats (APTs) to take advantage of poorly managed privileged accounts. The proliferation of privileged accounts beyond the data center to cloud-based infrastructure amplifies the complexities of securing privileged access to critical servers and network equipment.

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.

Implementing multi-factor authentication, securely managing remote access and shared account credentials and monitoring privileged sessions are at the root of reducing threats, intentional or not. And a comprehensive solution results in cost-effective regulatory compliance as a part of doing business.

Granular Control without a VPN

Centrify Privilege Service provides all of your IT administration teams with secure, granular access to infrastructure regardless of location, and without the hassles of a VPN.

Secure browser-based access

Authorized IT users launch management sessions for resources directly from the Privilege Service portal. Sessions use SSH and RDP protocols, and are always protected end-to-end.

Access across organizational boundaries

Privilege Service enables you to authenticate your IT users through Active Directory, LDAP Centrify Cloud Directory, or Google G Suite Directory. You can use one or any combination of these identity stores to grant granular access to employees, business partners and outside vendors.

Grant access to specific resources

Unlike a VPN, Privilege Service enables you to grant access to resources on a on a per-resource basis. This means that you can easily give your internal IT admins access to as much of your infrastructure as necessary, while limiting access by an outsourced team to only the servers and network hardware their business role or IT function requires.

Access from any location

Your IT admins can log in and securely access resources from any location that can reach the Privilege Service. For user logins outside the corporate network, you can require Centrify's built-in multi-factor authentication for security stronger than a user name and password.

Identity Flexibility for Hybrid Cloud Environments

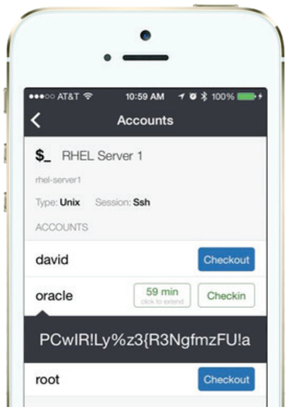
Centrify Privilege Service seamlessly connects servers deployed on-premises or in the cloud to an organization's identity provider of choice — including Active Directory and LDAP directories — without having to replicate complex identity infrastructure. Organizations can also leverage cloud-based directories such as the Centrify Directory or Google G-Suite Directory for Linux server authentication.

Streamlined adoption of IaaS

Centrify Privilege Service makes it easy to securely move infrastructure and apps to the cloud. Organizations take advantage of the benefits of the cloud without compromising the level of privileged access security and enterprise access they currently have on-premises.

Control Shared Access to Privileged Accounts

Centrify Privilege Service gives you control over shared accounts. Regardless of where your server and network infrastructure is located — on-premises or in the cloud — Privilege Service gives your IT admins secure, always-on access to critical shared account passwords, while giving you control over who has access, which account passwords they have access to, and how those passwords are managed.



$_ RHEL Server 1
rhel-server1
Type: Unix Session: Ssh
ACCOUNTS
david
oracle
PCwIR!Ly%z3{R3NgfmzFU!a
root

Reduce deployment and management costs

Simplify and automate shared account password management for super-user and service accounts with a single solution for hybrid IT that can be deployed as a service, in a private cloud or on-premises.

Secure checkout of account passwords

Authorized IT users can checkout passwords for accounts for a limited duration, displaying them or copying to the clipboard. Privilege Service delivers "break-glass access to passwords from mobile devices enrolled in the Centrify Cloud. Secured password checkout requires a PIN or fingerprint validation.

Automatic password resets

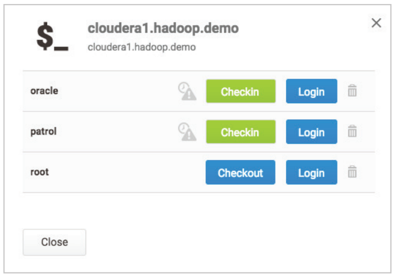
Privilege Service generates a new password and changes the password on the target system when a checkout expires. Complex, high-entropy passwords are created at run-time by Microsoft .NET cryptography libraries.

Remote sessions using shared accounts

In combination with the secure remote access features, authorized users log in to resources using shared accounts without Privilege Service disclosing the passwords to them.

Control access globally, per-resource, and per-account

Privilege Service provides you with both global and granular control of permissions for accounts and passwords. You have full control over who can access which resources, and which accounts they can use.



$_ cloudera1.hadoop.demo
cloudera1.hadoop.demo

oracle
patrol
root

Authorized users can launch management without knowing the password.

Reinforce Secure Access to Critical Systems

Privilege Service provides built-in multi-factor authentication (MFA) for session initiation and password checkout. In combination with Centrify Server Suite® Privilege Service also provides an extra layer of security to protect against hackers by configuring MFA for IT administrators who access UNIX and Linux systems and require elevated privileges.

Self-service Privileged Access Request

Minimize your attack surface with governed access to privileged account credentials and remote sessions. Keep control with request and approval workflows, time-bound access and privileged session monitoring. Capture who requested access and who approved it, and easily reconcile approved access with actual access for privileged access governance.

Secure, Encrypt and Manage Application Passwords

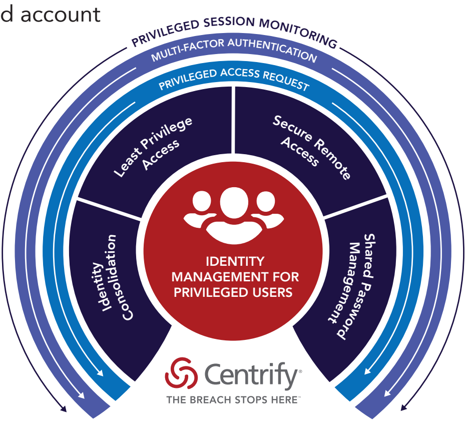
Prevent cyberattacks that target privileged account credentials and streamline operations by eliminating hard-coded, plain text account passwords from scripts and applications. Applications and scripts authenticate and retrieve passwords securely without human intervention, enabling organizations to meet compliance and security policies.

Monitor Privileged Sessions

Consistently monitor privileged sessions, whether using shared accounts or user accounts with privilege elevation, for servers and network devices, both on-premises and cloud-based. An audit add-on to Privilege Service provides gateway-based session monitoring, the ability to watch and terminate suspicious sessions and session reporting while Server Suite offers full host-based privileged session monitoring for additional security.

Identity Management for Privileged Users

Privilege Service complements Server Suite by delivering secure managed access and shared account password management for on-premises servers and network equipment as well as Infrastructure-as-a-Service (IaaS). Together they constitute Centrify's identity management for privileged users solution, which reduces the risk of security breaches by minimizing the attack surface and auditing all privileged sessions.



PRIVILEGED SESSION MONITORING
MULTI-FACTOR AUTHENTICATION
PRIVILEGED ACCESS REQUEST
Least Privilege Access
Secure Remote Access
Identity Consolidation
Shared Password Management
IDENTITY MANAGEMENT FOR PRIVILEGED USERS
Centrify
THE BREACH STOPS HERE

Benefits

- Eliminate identity-related risks associated with shared accounts
- Flexible deployment choices include a cloud service, or managing the solution entirely within your own data center or IaaS deployment.
- Mitigate the risks of granting full VPN access
- Secure privileged access for outsourced IT
- Lower TCO with a single, integrated solution

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**