CENTRIFY PRIVILEGED ACCESS SERVICE

Putting Core Privileged Access Controls in Place

Over the last few 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, default, stolen, or otherwise compromised privileged credentials. To add to this challenge, the attack surface of organizations has changed dramatically. Today, privileged access management is not only relevant for infrastructure, databases, and network devices, but extended to cloud environments, Big Data, DevOps, containers, applications, services, and more. Considering both internal and external identity-based threats, IT organizations must take a first step towards Identity-Centric PAM by vaulting away shared account and application passwords, as well as secrets. With the growth of mobile workforces, outsourced IT, and third-party contractors, it is also vital to ensure remote access is legitimate and isolate internal systems from external user devices to avoid infections during remote sessions.

Privileged Accounts are the Keys to the Kingdom

Data breaches are all over the news, perpetrated by malicious insiders as well as external hackers. Whether nation state-led espionage, encrypting data for ransom, or disabling critical servers, the methods used to gain privileged access are consistent. Unsubtle, guns-blazing, brute force hacking is for the history books. The method du jour is to simply log in using weak, default, stolen, or otherwise compromised credentials, exploiting the allowed permissions of legitimate employees to do illegitimate things. Once in, the hacker moves laterally from server to server, seeking greater privileges to help them gain access to the organization's most critical infrastructure and sensitive data.

Forrester Research has estimated that 80 percent of security breaches involve privileged access abuse and 66 percent of companies have been breached an average of five times.

In response, today's modern organizations must control and monitor privileged accounts and access for both internal and outsourced IT, while aiming to improve IT productivity rather than at its expense.

Putting Core Privileged Access Controls in Place

The Centrify Privileged Access Service allows organizations to establish core privileged access management (PAM) and security controls across an expanding number of attack surfaces. Vaulting away shared accounts for users, applications, and services as well as secrets used by for example DevOps, is a first step towards a comprehensive PAM posture. By taking them out of the wild and locking them down, you immediately reduce the attack surface and hence, your risk.

You're then able to better govern legitimate use, enabling secure remote access to servers and network devices using a VPN-less approach, workflow-based access request/approval for just-in-time access, time-boxed rights to avoid standing privileges, adaptive multi-factor authentication (MFA) for stronger identity assurance based on context or a risk score, and session recording for forensic-level incident response and compliance.

Simply vaulting passwords is not enough. Centrify Privileged Access Service manages them through capabilities such as remote login without password reveal, routine password rotation, password quality-of-service, and automatic password reconciliation.

SHARED PASSWORD MANAGEMENT

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

SECURE REMOTE ACCESS

Provide remote admins, outsourced IT, and third-party vendors with secure access only to the specific servers and network devices they manage, whether on-premises or in the cloud. Support VPN-less remote login sessions via browser or native client (e.g., PuTTY or Microsoft Remote Desktop app).

CREDENTIAL MANAGEMENT

To prevent cyber-attacks and meet audit and compliance requirements, secure and control access to vaulted passwords, SSH keys, and secrets based on policy. Automatically rotate passwords and reconcile out-of-sync passwords to ensure availability and reduce IT overhead.

ACCESS REQUEST & WORKFLOW APPROVAL

Minimize your attack surface by eliminating static rights. Enforce a just-in-time approach, whereby a user requests emergency password checkout or a remote login session (via Centrify, ServiceNow® or SailPoint Technologies® IdentityIQ workflow) only when needed. The approver grants access for a limited period after which, Centrify Privileged Access Service automatically revokes the additional roles. Log who approved access and reconcile approved access with actual access.

GATEWAY CONNECTORS FOR ISOLATION AND MULTI-CLOUD SCALE

Especially for outsourced IT, it is essential to isolate critical IT infrastructure from user workstations, ensuring a "clean source" to prevent the spread of viruses and malware. Distributed Gateway Connectors act as lightweight spokes, bridging your disparate networks into the Centrify Privileged Access Service hub. Drop in as many as you need to scale out rapidly in the data center, DMZ, multi-VPC, or multi-cloud.

MFA AT VAULT

To stop bots and malware in their tracks, and to better assure the identity of a human user, use MFA at vault login, password or secret checkout, and remote login session initiation.

Meeting Your Business Needs

Centrify Privileged Access Service was the industry's first native PAM-as-Service solution designed for modern, hybrid IT infrastructures. Customers can choose to consume this Centrify-managed SaaS service, or manage it themselves — deploying the same hyper-scalable software in their own data center or private cloud.

Irrespective of where the software lives, it's accessible from a Web browser for interactive use, but also has a complete set of RESTful APIs, UNIX/Linux command line interfaces (CLIs), PowerShell commandlets, and sample scripts for tools such as Terraform, Ansible, and Chef (on GitHub) used by DevOps, application-to-application password management (AAPM), and other automation processes.

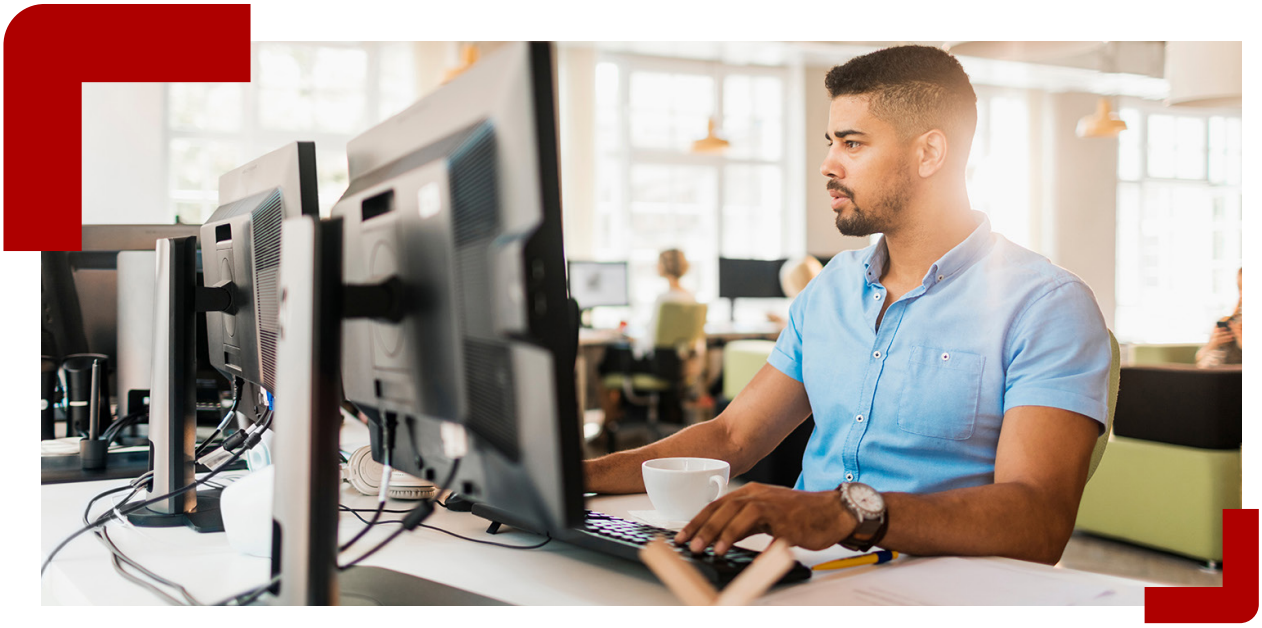
For convenience, a mobile app provides admins with emergency break-glass password checkout, secure certificate-based MFA, one-time-passwords, and workflow-based approvals.

The service even helps organizations 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).

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 as 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 governed, via access policy, for users, services, and applications. Key capabilities include:

- Scan Active Directory or network ports to discover Active Directory domains, Windows or UNIX servers, workstations, network devices, and to vault dash-a, local, and domain accounts associated with users, services, application pools, and scheduled tasks.
- Allow emergency "break-glass" checkout of account passwords, SSH keys, and secrets from a regular browser or a Centrify mobile app.
- Enable remote login via built-in Web client or using local client (e.g., PuTTY and Microsoft Remote Desktop), without disclosing passwords.
- Provide contextual and risk-based policies for checkouts and privileged sessions, invoking MFA as necessary.
- Rotate managed passwords automatically on a schedule, based on an event (e.g., check-in), or manually in bulk (e.g., in response to a breach).
- Reconcile vaulted passwords automatically, if they are out-of-sync with the local system password (e.g., if a privileged user manually changes it on the system).



Secure and Manage Application Secrets

Aside from credentials used by human admins, for DevOps, application-to-application passwords, and other automation scenarios, you can vault additional secrets such as IP addresses, SSH keys, and configuration settings. Applications and scripts can programmatically retrieve them via RESTful APIs, CLIs, or PowerShell cmdlets. Benefits include:

- Provide stronger security and increase compliance posture.
- Eliminate hard-coded passwords from scripts and applications.
- Secure application access to privileged account credentials.
- Centrally manage secrets to reduce overhead and sprawl.
- Rotate password automatically to minimize the risk of being compromised.
- Manage SSH keys (inclusive of key rotation), set policies for the SSH key rotation, and leverage an account that has an SSH key for system and account discovery operations.
- Reconcile out-of-sync passwords to avoid login failures, ensuring system availability and reducing IT and help desk overheads.
- Avoid manually establishing service accounts for each application by leveraging the local Centrify Client that can delegate its own credential. Subsequently, the applications can use the Centrify Delegated Machine Credential to authenticate to the Centrify Privileged Access Service and access its APIs.
- The Centrify Command Line Interface (CLI) provides quick and easy command line or scripted interaction with the Centrify Privileged Access Service's APIs, without the complexity of having to write REST client code.

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 the vault or leverage stronger federation technologies for client-to-server authentication, depending on what's best for the application. Centrify can issue short-lived tokens as a stronger alternative to static passwords. For even more security, you can leverage Centrify's built-in OAuth2 client to limit which APIs an application can invoke, helping to constrain access and mitigate the risk of hijacking.

- Centralized systems and service accounts.
- OAuth2 to grant limited access to resources without having to expose credentials.
- OpenID Connect for confidential client authentication.
- SAML tokens for Web access.
- Take advantage of client-based password reconciliation for local accounts. This allows for password resets, account unlock on Windows machines, password rotation, and many other account operations without having to rely on the Centrify Gateway Connector or more importantly without increasing the attack surface with extra privileged accounts.

"When you get a clear picture of the breadth of capabilities Centrify Identity-Centric PAM solution provide, you begin to understand just how many security check boxes it ticks. I'm still surprised at the number of issues I was able to address with just this single solution."

MATT HORN, IT OPERATIONS MANAGER, GSI

Document Actions for Forensic Analysis and Governance

Centrify Privileged Access Service allows you to record privileged sessions at the Gateway Connector and monitor sessions in real time via the UI, with the option to terminate them if needed.

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 their location or the location of your infrastructure. Keep them off the network and avoid the risks inherent in VPNs.

- Secure access to servers, network devices, and IaaS consoles such as AWS Management Console.
- Secure access for employees and third parties — remote and on-site — authenticated against Active Directory, LDAP, or cloud repositories such as Google or the Centrify Platform Directory.
- Limit unnecessary network and resource exposure by surgically placing the user on a specific target server or network device.
- Provide convenient break-glass access to passwords from a mobile app.

Eliminate the Potential for Workstation-related Infections

You can quickly deploy Centrify Gateway Connectors wherever your resources exist, as part of a scalable, distributed hub-and-spoke model. They isolate your infrastructure from the laptops and workstations used to remotely access them, ensuring a "clean source" by preventing the spread of any viruses or malware. This is especially beneficial for third parties and outsourced IT, where you have less physical control.

- Secure remote access to Windows, Linux, and UNIX servers as well as network devices using a local RDP or SSH client, or through the built-in Web client.
- Provide centralized visibility and access (depending on assigned roles) to all infrastructure resources irrespective of location (data center, DMZ, or IaaS providers).
- Configure and launch desktop apps that reside locally or on a remote application host system, such as SQL Server Management Studio, TOAD for Oracle, and VMware vSphere Client, as well as custom applications using the generic application template.

Self-Service Privileged Access Request and Approval Workflow System

To support just-in-time access, workflow-based self-service requests for access request can be made from the Centrify Privileged Access Service UI or optionally from ServiceNow and SailPoint Technologies IdentityIQ.

- Self-service request for password checkout, remote login, and privilege elevation (see Centrify Privilege Elevation Service).
- Leverage Centrify built-in access request and multi-level approval workflow or third parties (e.g., ServiceNow and SailPoint Technologies).
- Avoid standing privileges by requiring a duration, after which, Centrify Privileged Access Service automatically revokes the incremental rights.

Minimize Risk, Increase Assurance with MFA at the Vault

Centrify provides full service MFA capabilities built into the Centrify Platform itself, supporting the broadest array second factors as well as third party solutions that support standard protocols such as RADIUS, OATH, and FIDO2. MFA profiles enforce which second factors can be used, to help ensure compliance with more prescriptive regulations and industry recommendations such as NIST Authenticator Assurance Level 3, which requires a hardware cryptographic token.

- Native MFA support or integration with third-party solutions.
- MFA for vault login, checkout, and session initiation.
- Rule-based, contextual MFA policies or adaptive, risk-based.

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 with Identity-Centric PAM based on Zero Trust principles. 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

www.centrify.com