Centrify
ZERO TRUST PRIVILEGE

Mission Possible: More Secure. More Compliant.

Minimize the Attack Surface and Control Privileged Access with Centrify Zero Trust Privilege Services

Government agencies hold a vast amount of sensitive information, ranging from personnel records, budgetary data, inter-community communications to intelligence findings related to terrorists and hostile nations. In turn, governments all over the world are continually under threat of complex, sophisticated attacks launched by rival nation-states, terrorist groups, hacktivists, and cyber criminals. In addition, they are facing insider threats as showcased by Edward Snowden. Trusted by top government agencies, Centrify Zero Trust Privilege solutions help tackle the #1 cause of today's breaches — privileged access abuse.

Increase Security and Compliance Posture

A compromise of government data could jeopardize national security and undermine public safety. Thus, government agencies, be it on the Federal, State, or Local level, have cyber security top of mind. To provide guidance, the National Institute of Standards and Technology (NIST) has developed a variety of frameworks and guidance, which are published in the NIST Special Publication 800-Series.

In addition, government IT staff must find the right balance between security (as mandated by federal, state and local regulations) with end user productivity. Ultimately, government IT's priority is to support the agency's mission, and not necessarily spend too much time on annual reviews and cumbersome reporting requirements.

Let Us Help You

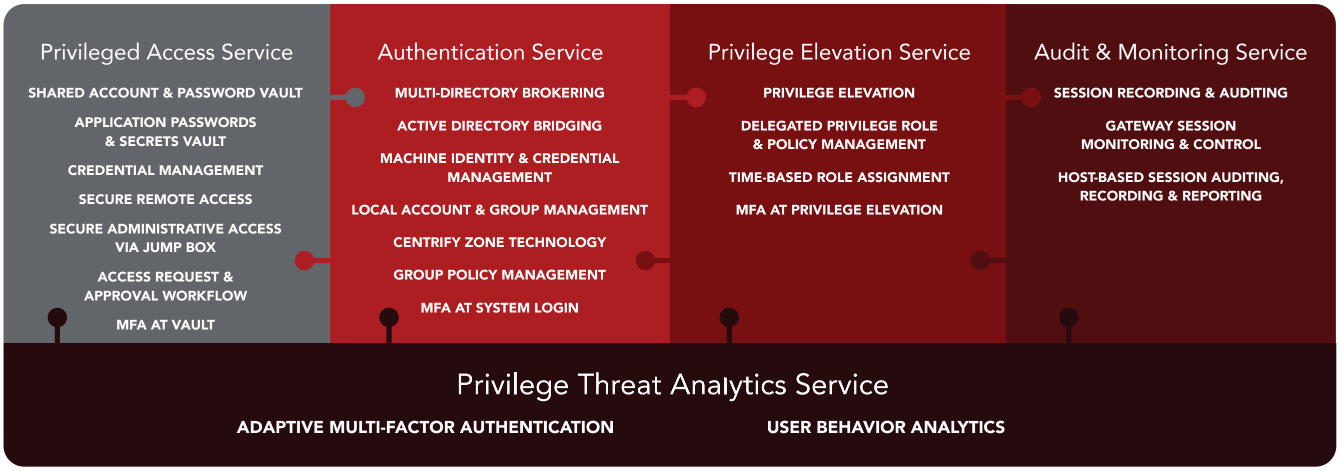
Centrify has you covered when it comes to securing privileged access to your infrastructure. In addition, Centrify Zero Trust Privilege solutions help government agencies assure continuous transparency into their compliance posture, addressing key regulations and industry standards such as CIS, CJIS, DHS CDM Phase 2, FERPA, FICAM, FISMA, HIPAA, HITECH, HSPD-12, NIST SP 800-Series, OMB, PCI DSS, etc.

Meet the Antidote to Privileged Access Abuse: Zero Trust Privilege

Centrify Zero Trust Privilege combines password vaulting with brokering of identities, multi-factor authentication (MFA) enforcement, and "just enough, just-in-time" privilege, all while securing remote access and monitoring all privileged sessions.

The Centrify Privileged Access Service has received authorization by the U.S. Government's Federal Risk and Authorization Management Program (FedRAMP). Sponsored by the Overseas Private Investment Corporation (OPIC), this authorization allows government agencies to adopt Centrify's cloud-ready service for Privileged Access Management (PAM) and bolster mission security as they migrate an increasing number of workloads to the cloud. Check out the FedRAMP Marketplace listing for more details. The FedRAMP Authorized Centrify PAS seamlessly integrates with Centrify's other solutions, namely the Centrify Authentication Service (which helps verify who requests privileged access by leveraging enterprise directory identities rather than local accounts) and Centrify Privilege Elevation Service (which enables host-based enforcement of just enough, just-in-time privileged access best practices).

CENTRIFY ZERO TRUST PRIVILEGE SERVICES



Privileged Access Service
- SHARED ACCOUNT & PASSWORD VAULT
- APPLICATION PASSWORDS & SECRETS VAULT
- CREDENTIAL MANAGEMENT
- SECURE REMOTE ACCESS
- SECURE ADMINISTRATIVE ACCESS VIA JUMP BOX
- ACCESS REQUEST & APPROVAL WORKFLOW
- MFA AT VAULT

Authentication Service
- MULTI-DIRECTORY BROKERING
- ACTIVE DIRECTORY BRIDGING
- MACHINE IDENTITY & CREDENTIAL MANAGEMENT
- LOCAL ACCOUNT & GROUP MANAGEMENT
- CENTRIFY ZONE TECHNOLOGY
- GROUP POLICY MANAGEMENT
- MFA AT SYSTEM LOGIN

Privilege Elevation Service
- PRIVILEGE ELEVATION
- DELEGATED PRIVILEGE ROLE & POLICY MANAGEMENT
- TIME-BASED ROLE ASSIGNMENT
- MFA AT PRIVILEGE ELEVATION

Audit & Monitoring Service
- SESSION RECORDING & AUDITING
- GATEWAY SESSION MONITORING & CONTROL
- HOST-BASED SESSION AUDITING, RECORDING & REPORTING

Privilege Threat Analytics Service
- ADAPTIVE MULTI-FACTOR AUTHENTICATION
- USER BEHAVIOR ANALYTICS

Centrify Privileged Access Service

The Centrify Privileged Access Service provides you with all the capabilities to achieve your first step toward Zero Trust Privilege.

- Discover and register all your privileged accounts and resources (including workstations) and vault away those privileged credentials so that they are properly managed.
- Provide remote admins, outsourced IT, and third-party vendors with secure, VPN-less access to the specific infrastructure they manage — on-premises and in the cloud.
- Leverage a locked down and clean server gateway that serves as a distributed local jump box to avoid infections during remote connections.
- Govern access to privileged account credentials, privileged sessions, and roles that grant privilege to individuals, with approval workflows.
- Monitor and record privileged sessions at the gateway level and terminate them if needed.
- Apply MFA everywhere. This applies during vault login, password checkout, and server login.

Centrify Authentication Service

Cloud-ready Zero Trust Privilege is designed to handle requesters that are not only human but also machines, services, and APIs.

There will still be shared accounts, but for increased assurance, best practices now recommend individual identities and short-lived tokens, not shared accounts and static credentials.

- Simplify user authentication to servers from any directory service including Active Directory, LDAP, and cloud directories.
- Secure Linux and UNIX with the same identity services currently used to secure access to Windows systems.
- Centrally manage machine identities and their credentials within Active Directory or the Centrify Authentication Service to establish an enterprise root of trust for machine-to-machine authentication based on a centralized trust model.
- Manage system accounts the same way you would manage user accounts in Active Directory.
- Quickly consolidate complex and disparate UNIX and Linux user identities into Active Directory with Centrify's patented Zone technology — without having to first rationalize all user identities.
- Manage authentication, access control, and group policy for non-Windows systems the same way as Windows.
- Multi-factor authentication at login for Linux, UNIX, and Windows servers minimizes the risk of exposure.

Centrify Privilege Elevation Service

Centrify Privilege Elevation Service minimizes the risk exposure to cyber-attacks caused by individuals with too much privilege. The service allows customers to implement just enough, just-in-time privileged access best practices and in turn limit potential damage from security breaches.

- Secure and manage fine-grained privileges across Windows and Linux systems, limiting potential damage from security breaches via privilege elevation.
- Simplify management of roles, rights, and privilege policies across heterogenous (UNIX, Linux, and Windows) systems.
- Minimize security risk by enabling administrators to systematically request a new role to obtain the rights they need to perform tasks.
- Protect the execution of a privileged command through MFA.

Centrify Audit and Monitoring Service

For privileged sessions it is best practice to audit everything. With the Centrify Audit and Monitoring Service, monitoring and session recording can be achieved through a gateway-based and/or host-based technique. Advanced monitoring capabilities even allow for process launch and file integrity monitoring.

- Record and manage a holistic view of privileged activity across Windows and Linux servers, IaaS, and network devices, establishing a single source of truth for individual and shared accounts.
- Gain new levels of oversight for privileged sessions on critical infrastructure. Administrative users watch activity in remote sessions in real-time and can instantly terminate suspicious sessions through the Centrify Admin portal.
- Ensure session recording cannot be bypassed, with host-based auditing. Discover rogue activity such as the creation and storage of SSH key pairs that would make it easy to bypass security controls, and attribute activity to the individual user.

Centrify Privilege Threat Analytics Service

Cyber adversaries are getting more and more sophisticated and therefore it is best practice to apply multiple security layers when protecting against privileged access abuse. Today's threatscape requires security controls to be adaptive to the risk-context and to use machine learning to carefully analyze a privileged user's behavior. Leveraging Centrify Privilege Threat Analytics Service can make the difference between falling victim to a breach or stopping it in its tracks.

- Add an extra layer of security to stop the breach with risk-aware, adaptive MFA for IT admins who access Windows and Linux systems, elevate privilege, or leverage privileged credentials.
- Leverage modern machine learning algorithms to carefully analyze a privileged user's behavior and identify "anomalous" or "non-normal" and therefore risky activities and alert or notify security. In addition, privileged user behavior analytics can be used to analyze most used and least used commands and activities and serve as a governance function to suggest changes to roles and rights.

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®

www.centrify.com