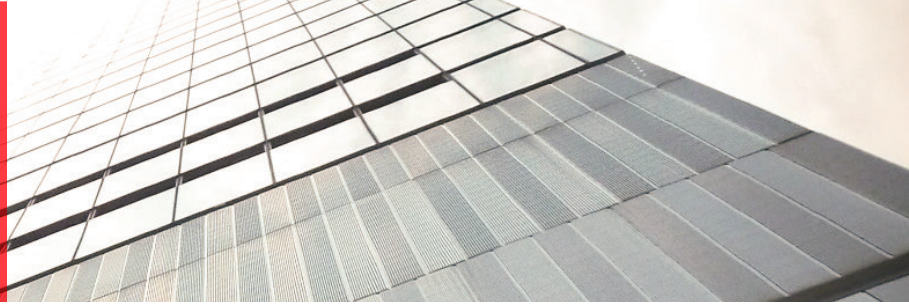
Centrify
ZERO TRUST PRIVILEGE



Centrify Privilege Elevation Service

Establish Least Privilege Access to Reduce the Attack Surface

Over the past few years, it's become evident that attackers are no longer "hacking" in for data breaches: they are simply logging in using weak, stolen, or otherwise compromised privileged credentials. Once they are in, they take advantage of the fact that many organizations assign too much privilege to their administrative users. This allows hackers to 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. Zero Trust Privilege mandates to grant just enough, and just-in-time privilege to limit lateral movement across the network.

Danger Zone: Too Much Privilege

Least privilege as a concept is more common than you realize. Think of physical access control at your office: different levels of users have different access rights, and to get access to certain areas you must request and be approved. This is all very well recognized in the physical security space, and the same logic applies for logical security. It applies when granting granular role-based access to privileged resources.

Another objective to granting least privilege is to limit lateral movement across the network. This is the primary way attackers get access to sensitive data: they start in one location and move laterally until they find what they are looking for. If we zone off what they have access to then we can stop lateral movement. Just like nobody should have a single key/badge that accesses everything, you really don't want to use the root account on a server, as it gives too much access and has no attribution to the actual user, who we'll call "Bob." Instead, Bob should login directly to the target system with his own admin entitlements that give him access to restart only a particular set of servers. If he needs to change the configuration, or access a different target system, then he must request access for a specified period of time. Access can be provisioned automatically or through something like ServiceNow® or SailPoint Technologies®. In addition, he may be asked for multi-factor authentication (MFA). Once complete, Bob's entitlements will reduce back to just what is needed.

Establish Least Privilege Access to Reduce the Attack Surface

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, limiting potential damage from security breaches.

PRIVILEGE ELEVATION

Secure and manage fine-grained privileges across Windows, Linux, and UNIX systems, limiting potential damage from security breaches. Get users to login as themselves for accountability, and elevate privilege based on their role within an organization.

TIME-BASED ROLE ASSIGNMENT

Minimize security risk by enabling administrators to systematically request a new role to obtain the rights they need to perform tasks. Access request for privileged roles enables organizations to grant long-lived or temporary privileges and roles with a flexible, just-in-time model that accommodates fluctuating business needs.

DELEGATED PRIVILEGE ROLE & POLICY MANAGEMENT

Centralized roles, rights, and privilege policies simplify management across heterogeneous (UNIX, Linux, and Windows) environments. Policies are stored in Active Directory separate from other common objects to support delegation to server administrators and separation of duties from Active Directory administrators, preventing server admins from managing Active Directory objects they should not. All of this is done without Active Directory schema modifications.

MFA AT PRIVILEGE ELEVATION

MFA at login is a great best practice — especially for administrators. However, it should be augmented with MFA at privilege elevation to protect from malicious actors by ensuring only authorized humans are launching privileged commands through MFA validation prior to privileged command execution.

Grant Just Enough Privilege Across Windows, Linux, and Unix

Reduce the risk of attack through individuals with too much privilege and routine use of shared privileged accounts. Implementing least privilege access limits potential damage from security breaches. Thus, the flexible, fine-grained Centrify Privilege Elevation Service lets your users get work done, reduces risk, and makes implementing a just-in-time, least privilege model easy with role-based access controls.

- Role-based access controls make least privilege easy. Centrify's patented Zones Technology provides highly granular, role-based access controls that simplify the implementation of a least privilege model across Windows, Linux, and UNIX systems.
- Secure your Windows, Linux, and UNIX systems by controlling exactly who can access what and when. Unlike de-centralized single-purpose tools like sudo, Centrify enables the configuration of dynamic privileges so that users can only elevate privilege at specific times, for a length of time, and on certain servers. You can also isolate servers based on time and trust relationships to further protect sensitive data. This helps limiting lateral movement further.
- Centrify provides a powerful set of tools to simplify adoption and management of a least privilege access model.

Simplify the Management of Heteregenous Environments

Centralized roles, rights, and privilege policies simplify management across heterogeneous (UNIX, Linux, and Windows) environments. Centrify Zero Trust Privilege Services policies are stored in Active Directory separate from other common objects to support delegation to server administrators and separation of duties from Active Directory administrators, preventing server admins from managing AD objects they should not. In addition, Centrify provides a hierarchical policy model designed to support common enterprise management models for top-down centralized control with centrally managed common roles and rights while also supporting departmental, role-based, and computer-based delegation to subordinate administrative teams for rights assignments to systems.

- Consistent and structured policy model for both Windows, Linux, and UNIX enables compliance and lower cost of maintenance.
- Managing both Windows, Linux, and UNIX policy in Active Directory enforces a consistent approach towards privileged access security and in addition, creates the proper separation of duties between policy owners and system administrators. This homogeneous approach to heterogeneous environments ensures shorter audits and eases compliance.

Self-Service Role Requests for Just-In-Time Privilege

Minimize security risk by enabling administrators to systematically request a new role to obtain the rights they need to perform tasks. Access request for privileged roles enables organizations to grant temporary privileges and roles with a flexible, just-in-time model that accommodates fluctuating business needs.

- Enable administrators to log in as themselves and elevate privilege by systematically requesting a new role assignment to obtain the rights they need to perform tasks. A self-service request system facilitates the request for the specified role and time period, and if approved will automatically revoke that entitlement upon expiration.
- Minimize the attack surface by enabling temporary, and time-bound access to privileged accounts and privileged roles for just-in-time privilege. Grant IT admins access to privileged account credentials, remote management sessions, or when they need to temporarily modify their role assignment for performing additional admin tasks.
- Reduce the risk of data breaches by requiring approval for IT users who need access to systems with privileged roles. IT users of the ServiceNow® asset management and configuration management database (CMDB) or SailPoint Technologies® identity governance and administration solutions can request usage of a role with privileges to access specific servers for a designated time period. Approvals are granted or denied through a workflow-based management process.

Validate That the Proper Privileged User is Launching Privileged Commands

The execution of a privileged command should always be protected from malicious actors by ensuring only authorized humans or only applications and services with appropriate rights can perform privileged activity. Centrify provides host-based technology, which cannot be circumvented to enforce MFA upon privileged execution across Linux, UNIX, and Windows servers.

- Whether you apply MFA at system or vault login, or during privilege elevation, integration with the Centrify Privileged Access Service allows a consistent and easily maintainable MFA service for all privileged access. With the broadest range of authenticators and out-of-the-box support for NIST Level 2 and 3 Assurance Levels.
- A Zero Trust Privilege approach requires always verifying who is requesting privileged access. UNIX/Linux admins logging in to check the system is not considered risky and should not require MFA, however execution of any privileged commands should be configured to require MFA prior to execution leveraging Centrify's centralized MFA services.
- A Zero Trust Privilege approach requires always verifying who is requesting privileged access. Windows admins who need to execute privileged commands can be challenged for MFA, required to reauthenticate with their AD password, or validate their identity with a smart card.

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