Centrify

ZERO TRUST PRIVILEGE

BECOMING PCI DSS COMPLIANT

www.centrify.com

ABOUT CENTRIFY

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise use cases. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid enterprise. Over half of the Fortune 100, the world's largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Centrify to stop the leading cause of breaches — privileged credential abuse.

To learn more visit www.centrify.com.

Centrify's mission is to stop the leading cause of breaches – privileged access abuse. Centrify empowers organizations with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise attack surfaces. Centrify Zero Trust Privilege helps grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid enterprise.

Centrify Zero Trust Privilege Services enable organizations to consolidate identities, deliver cross- platform least privilege access, and control shared accounts while securing remote access and auditing all privileged sessions. In turn, Centrify helps address many of the PCI DSS requirements concerning privileged account management and usage, as well as control over access to resources that are in scope of PCI DSS.

Abstract

The Security Standards Council of the Payment Card Industry (PCI) owns and maintains the Data Security Standard (DSS), a rigorous set of requirements that all merchants, payment processors, point-of-sale vendors, and financial institutions must follow. The stiff penalties defined by PCI members are designed to ensure that all merchants and service providers work to maintain consumer trust of payment cards, since loss of that trust could negatively impact revenue.

The PCI DSS 3.2 consists of 12 requirements spread across six domains. Since the core concern of PCI is the protection of cardholder data, these requirements focus on privileged user access to the servers that host this data, or through which such data passes.

This white paper examines each of the 12 requirements and identifies the associated Centrify Zero Trust Privilege Services capabilities that customers can leverage to help achieve compliance.

PCI Requirements Applicability Summary

Centrify Zero Trust Privilege Services contribute to your PCI DSS compliance posture in several different areas. They provide security controls to manage and constrain privileged user access to PCI DSS systems and data. They can also help reduce PCI scope by isolating PCI resources, controlling user access, server-to-server communication (i.e., their communication to untrusted servers), and the encryption of data between them. One other key aspect is that Centrify Zero Trust Privilege Services are cross-platform, giving you centralized control and visibility across Windows, Linux, and UNIX.

The table below provides a high-level view of the domains/requirements where Centrify Zero Trust Privilege Services contribute to achieving PCI DSS compliance.

PCI Domain	Requirement	Centrify Zero Trust Privilege Services
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	YES
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	YES
Protect Cardholder Data	3. Protect stored cardholder data	YES
	4. Encrypt transmission of cardholder data across open, public networks	YES
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs	N/A
	6. Develop and maintain secure systems and applications	YES
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	YES
	8. Identify and authenticate access to system components	YES
	9. Restrict physical access to cardholder data	N/A
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	YES
	11. Regularly test security systems and processes	YES
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	YES

PCI Requirements

#	Requirement	Centrify Zero Trust Privilege Services
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.		
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	**Centrify Zero Trust Privilege Services** provide group policy-based enforcement of an IP tables-based firewall. By using this policy, administrators can restrict inbound traffic to specific ports from specific IP addresses. **Centrify Zero Trust Privilege Services via its isloation and encryption capabilities** provide additional protections for the server by requiring authentication before any communication. This can be applied to both inbound and outbound communications to ensure PCI systems are only able to communicate with other PCI systems. **Centrify Zero Trust Privilege Services via its secure remote access capabilities** support VPN-less remote connectivity. An outbound persistent connection to the Centrify Identity Platform service ensures that additional firewall ports do not need to be opened.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	When mutual authentication is required, **Centrify's isolation and encryption capabilities** will prevent communication with untrusted systems or any system outside the network, as they cannot authenticate and are not trusted. **Furthermore, Centrify isolation and encryption capabilities** enforce the most secure form of network firewall protection, ensuring that a computer will only allow communications with other trusted systems. Additionally, Centrify can restrict remote access to servers based on role membership and login or password checkout for accounts on cardholder data systems can be explicitly denied or granted via a workflow-based approval process as required.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	**The Centrify Shared Account and Password Vault** stores shared privileged account passwords in a secure vault. Once these passwords are brought under management, Centrify will cycle the passwords from their default. Leveraging our REST APIs, Centrify provides sample scripts that are used by IT/DevOps to automate many tasks when standing up new servers on-premises or in IaaS. For example, these scripts can be used with orchestration tools (e.g., Chef, Puppet, OpsWorks) to automatically deploy Centrify software, install, configure, and join to AD and vault default accounts as described above.

#	Requirement	Centrify Zero Trust Privilege Services
2.3	Encrypt all non-console administrative access using strong cryptography.	While Telnet is in use on many systems, it is not secure and should be replaced with SSH, which provides for network transport security. Newer versions of OpenSSH support Kerberos for user authentication, and when combined with **Centrify Zero Trust Services**, eliminates the need to manage static SSH keys. Centrify also provides a compiled and easy-to-install version of the latest OpenSSH, enabling customers to ensure they have a consistent version across all their systems for the highest level of security. All privileged shared account sessions to resources are encrypted. From the privileged user's browser to the on-premises Centrify Connector via HTTPS and then via SSH or RDP to the end-point. Alternatively, users may initiate a secure SSH or RDP session directly from their local systems. In addition, Centrify supports risk-aware, two-factor authentication for privileged users logging into the Centrify admin portal to circumvent (e.g., pass) the hash attacks. Centrify also enables secure remote access without a VPN. While VPN traffic can be secure, it imposes other risks to the environment by allowing remote users broader access beyond the target server for which they need log in access. It is well-documented that cyber attackers target outsourced IT company users so they can use their VPN credentials as a "legitimate" user.
Requirement 3: Protect stored cardholder data		
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Centrify can grant/deny privileged activities using roles and rights maintained independent of the local operating system, in Active Directory.

#	Requirement	Centrify Zero Trust Privilege Services
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.	**Centrify Zero Trust Privilege Services via its isolation and encryption capabilities** provide IPsec-based integrity and confidentiality services at the network layer to encrypt all communications between any application on the system and other trusted remote hosts. Since this solution provides encryption services at the network layer, there is no need to modify any application to support this level of data protection. All privileged, shared account sessions to resources are secured over SSH or RDP. In addition, Centrify supports risk-aware, two-factor authentication for users logging into the admin portal to circumvent (e.g., pass) the hash attacks.
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**Centrify Zero Trust Privilege Services** can contribute to the overall reduction in potential virus attacks and are an effective complement to anti-virus solutions. A very common use case involves internal IT or outsourced third-party remote access to PCI servers via a VPN connection. Using this approach, there's the inherent risk of viral infection since the user computer is network-attached. **Centrify Zero Trust Privilege Services via its secure remote access capabilities** support VPN-less remote access wherein the remote user's computer is not network- attached. Instead, the remote session is established through a secure browser-based HTTPS connection, designed specifically to accommodate remote login scenarios in a more secure fashion than traditional VPN-based methods. Users are provided access to the specific target server instead of the broader network, sub-network, or jump-box, and since the user's computer is not network-attached, Centrify reduces exposure and obviates the potential risks of an infected computer spreading viruses or malware.
Requirement 6: Develop and maintain secure systems and applications		
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	The addition and removal of specific accounts is typically a function of third-party IAM products from vendors such as IBM, CA Technologies, and Oracle. However, with such accounts being under Centrify management, we can ensure they are securely encrypted, stored, and used only in line with appropriate access controls in a least privilege model. In addition, a common approach by IT/DevOps is to use orchestration tools such as Chef, Puppet, and OpsWorks to automate the configuration of new (virtual) servers. In this case, Centrify's REST-based APIs and sample scripts can be used to automatically join the computer to the Centrify Zero Trust Services and automatically vault any default accounts that can't be removed, putting the passwords under management and automatically rotating them.

#	Requirement	Centrify Zero Trust Privilege Services
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	The addition and removal of specific accounts is typically a function of third-party IAM products from vendors such as IBM, CA Technologies, and Oracle. However, with such accounts being under Centrify management, we can ensure they are securely encrypted, stored, and used only in line with appropriate access controls in a least privilege model. In addition, a common approach by IT/DevOps is to use orchestration tools such as Chef, Puppet, and OpsWorks to automate the configuration of new (virtual) servers. In this case, Centrify's REST-based APIs and sample scripts can be used to automatically join the computer to the **Centrify Zero Trust Privilege Services** and automatically vault any default accounts that can't be removed, putting the passwords under management and automatically rotating them.
6.4	Follow change control processes and procedures for all changes to system components	**Centrify Zero Trust Privilege Services** use Centrify Zones to create logical groupings of systems that have a discrete set of users, administrators, and policies. They restrict access methods and privileges based on job role. This can be used to provide separation between development, test and production machines to clearly separate groups of systems and their access permissions from each other. This model also works well to isolate development systems from production, helping to avoid the movement of test data to the production systems. **Centrify Zero Trust Privilege Services via its isolation and encryption capabilities** secure sensitive information by dynamically isolating and protecting cross-platform systems, and enabling optional end-to-end encryption of data in motion. It also leverages IPsec in transport mode for network security, which is applied to each packet individually, leveraging PKI credentials to establish unique session authentication keys for each security association. Centrify supports a role-based access control model that ensures users are only able to perform functions (remote login, password checkout, granting permissions) appropriate to their role. This governs user authentication to a specific account. Once logged in, Centrify can then govern authorization (i.e., specific access). To gain more control over access with just-in-time privilege for just-enough privilege, Centrify's workflow-based **privileged access request** can be used. Users can request membership to a defined role for more access, rights to login or checkout a password. **Centrify Zero Trust Services via its privileged access request capabilities** provide a multi-level approval process, where a combination of manager and approvers can grant or deny requests, with the option to grant permanently or temporarily.

#	Requirement	Centrify Zero Trust Privilege Services
6.4.2	Separation of duties between development/ test and production environments.	Per 6.4, above, Centrify's patented Zone Technology allows for separation of duties by constraining administrator access to specific resources. This enables for example a set of development servers to be grouped along with the administrators who can login to them, and further with a set of access rights on those systems, and other groups of resources such as test and production.
Requirement 7: Restrict access to cardholder data by business need to know		
7	Restrict access to cardholder data by business need to know.	Centrify implements a just-in-time privilege model for least privilege access, where users login with their own account and explicitly request privilege elevation to perform discrete administrative tasks. Such requests are granted or denied based upon need to know (i.e., a role-based access control model) centrally managed through Active Directory. This practice significantly reduces the threat surface by avoiding direct login and allowing most shared privileged accounts to be disabled, and ensures individual accountability. In addition, since access requests are made explicitly versus alternative approaches that intercept every single user action, check the policy and then apply the resulting action, Centrify has much lower impact on system resources and can perform session recording selectively instead of capturing the entire session, reducing resource overhead and simplifying audit and security investigation activities. **Centrify Zero Trust Services via its privileged access request capabilities** provide just-in-time privilege and just-enough-privilege by requiring role assignment approvals for privileged access requests. Admins configure multi-level approval workflows that ensure managers and other approvers review and approve access before access is granted. A complete audit trail improves privileged access governance by capturing who requested access, their business need, and who approved it. Centrify can restrict remote access to CDE resources to comply with business need to know. Users are granted the ability to login to accounts on resources and checkout account passwords only if they have the necessary roles, rights, and/or policies. Multi-factor authentication for privileged access can also be selectively enabled to provide additional identity assurance during login, password checkout, and privilege elevation.

#	Requirement	Centrify Zero Trust Privilege Services
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Centrify uses patented **Zone Technology** to control which users are granted access to specific systems. By default, Centrify enforces a Zero Trust model, i.e., Active Directory users do not have permissions to log into any managed system. However, by adding a user to a Centrify Zone and creating a UNIX profile for that user within Active Directory, the user will be granted access to those computer systems that are members of that same Centrify Zone. This results in a configuration where Centrify can show visually, as well as through reports which users have access to specific systems across the entire enterprise (on-premises or in the cloud). Additionally, Active Directory groups can be used within a pam.allow configuration rule within Centrify to further restrict which users within a given Centrify Zone can login to that specific system. The pam.allow and pam.deny configuration settings can be used to restrict access for individual users or groups of users. Active Directory Group Policy can also centrally control these rules. Active Directory also provides a profile setting for each user that allows an administrator to define a specific list of computers that the user can access. With **Centrify Zero Trust Privilege Services**, all non-Windows systems have a valid computer account within Active Directory, which enables administrators to define Windows and non-Windows systems in this list of allowed computers. These rules can all be applied to define the exact access control policy required for the specific computer. **Centrify Zero Trust Privilege Services** support a role-based access control model that ensures users are only able to perform functions (remote login, password checkout, granting permissions) appropriate with their role. This governs user authentication to a specific account. Once logged in, Centrify can govern authorization (i.e., specific access). Finally, **Centrify Zero Trust Privilege Services** use roles to govern which users can login to which resources (servers and network devices).
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:	Centrify supports a Zero Trust model whereby users do not have access to resources and cannot elevate privileges until explicitly granted. **Centrify Zero Trust Privilege Services** enable administrators to centrally manage a user's UNIX UID and group memberships, which are then used by the operating system to control user access to specific files and applications. To enable tighter controls around privileged operations, **Centrify Zero Trust Privilege Services** provide a Group Policy to enable centralized management of sudo permissions to ensure that the appropriate permissions are applied to local accounts in a consistent manner across the computers where this privilege should be granted. (continued next page)

#	Requirement	Centrify Zero Trust Privilege Services
7.2 (cont)	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following:	Centrify extends this functionality to define a set of Roles that will be granted specific access and privileged command rights. These Roles are defined on Active Directory enabling both AD users and AD groups to be assigned to the Role, simplifying ongoing management. These tools also serve to produce an audit trail of all privileged operations since sudo will log all command execution where the simpler "su" command does not provide this level of visibility, nor does allowing a user to login as the root account. Centrify also provides a mechanism to control the "root" account password policy through Active Directory to further protect those accounts that would otherwise be able to gain unbridled access to a non-Windows system. By default, Centrify disables all remote access to shared privileged accounts under management. Access must be explicitly granted by the tenant administrator.
7.2.1	Coverage of all system components	**Centrify Zero Trust Privilege Services** govern access to servers, network devices and specific applications/commands on Windows, Unix, and Linux servers within scope of PCI DSS, per 7.2, above.
7.2.2	Assignment of privileges to individuals	Per the capabilities outlined in 7.2, above, **Centrify Zero Trust Privilege Services** support role-based access control mechanisms that govern login to in-scope resources as well as privileges based on roles that map to a job classification and function per 7.2, above.
7.2.3	Default "deny-all" setting.	Per the capabilities outlined in 7.2, above, **Centrify Zero Trust Privilege Services** support a Zero Trust model whereby users do not have access to resources and cannot elevate privileges until explicitly granted access and rights to do so.

#	Requirement	Centrify Zero Trust Privilege Services
Requirement 8: Assign a unique ID to each person with computer access		
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.	**Centrify Zero Trust Privilege Services** support management of Windows, Unix, and Linux identities centrally within Active Directory, allowing companies to tear down identity silos that result in rogue accounts and privilege creep. AD is also used to apply roles and privileges to users and computers, to ensure consistent role-based access control across all systems. Further, it extends AD's group policy model to non-Windows systems for easier management and more consistent and comprehensive application of privileges. See below for additional details.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	UNIX systems have limitations such as maximum length of the login name that make it very difficult for IT staff to establish policies to ensure that an account is unique. Additionally, it can be challenging to identify the actual person that owns a specific UNIX account due to the default account database limitations that simply do not provide this ability. By using Active Directory, all users have a single, globally unique Active Directory account that Centrify subsequently links to each user's specific UNIX profile, which eliminates any ambiguity about who owns a specific UNIX account or the files created by that account. In some deployments, different groups of UNIX systems may have a local UID name space that overlaps with other groups of systems within the environment. Centrify Zones provide the ability to allow a user to have more than one UNIX profile for each of these groups of UNIX systems, thus eliminating any account or file ownership ambiguity while at the same time preserving access control integrity. Additionally, Centrify enforces uniqueness of its identities — those used to log in to the **Centrify Zero Trust Privilege Services** portal itself. Thus, all privileged activities (such as shared privileged account password checkout and remote sessions) are tied back to a unique user, ensuring individual accountability.
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Centrify user account administration is centrally managed within Active Directory, which provides a robust environment to delegate the administration of user accounts to the appropriate Active Directory administrator. Centrify extends this delegated administration to support the delegation of UNIX profile management to the appropriate UNIX administrator without requiring Active Directory administrators to grant elevated privileges within Active Directory. The result is an environment where UNIX administrators are enabled to grant or deny access to UNIX systems, but do not have the right to create a new user within Active Directory Additional controls are provided to prevent Active Directory administrators from creating a UNIX profile, which would result in a UNIX user with elevated privileges.

#	Requirement	Centrify Zero Trust Privilege Services
8.1.3	Immediately revoke access for any terminated users	Terminated user accounts are controlled through Active Directory, and upon Active Directory account termination, disabling or deletion, Centrify immediately refuses user login. Centrify can leverage Active Directory as its user store. Users revoked within Active Directory will not be able to login to the **Centrify Zero Trust Privilege Services** portal. If portal users are maintained in Active Directory, LDAP, or in the Centrify Directory, a customer can leverage its IAM Provisioning tool to de-provision from these repositories via (e.g.) LDAP or SCIM.
8.1.4	Remove/disable inactive user accounts within 90 days	Inactive user accounts are controlled through Active Directory, where Centrify properly updates the last login time for the user's Active Directory account to determine which accounts have not been used within 90 days. It's up to the administrator of the domain to manually ensure that inactive users are removed from it. In addition, roles and policies can be used to time-bound user access to resources. Roles can be configured to be only active during specific date/time ranges or with a defined revocation date. In addition, temporary rights to login to a resource or checkout a resource account password can be granted by a designated approver in response to a user access request.
8.1.5	Manage IDs used by vendors third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use; monitored when in use	Active Directory provides both a time-of-day restriction as well as an account termination date, which can be used to restrict an account's ability to be used for login to all systems. Centrify also provides a control to enable the UNIX administrator to selectively enable and disable a user's specific UNIX profile. This can be useful when a user needs periodic access to a group of UNIX systems. Roles can also be time-boxed to ensure they can only provide specific access rights during prescribed days of the week and times of the day. Centrify provides policies that govern specific users, their login to the admin portal (including via multi-factor authentication), and the resources they access. Policies can be established that disable accounts when not in use and enable them when in use. Temporary grants can also be assigned that grant login access or password checkout for a period of time, after which the rights are revoked.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts	Account lockout policy is set within Active Directory and can be set to lock out accounts after a specified number of invalid login attempts. Centrify enforces this policy on non-Windows systems. Since Centrify manages passwords on behalf of users there will be no invalid login attempts. Some use cases (e.g., "break glass") result in the password being revealed to an admin for interactive login. In this case, AD account logout policy can be set to lock out accounts after a specified number of invalid login attempts.

#	Requirement	Centrify Zero Trust Privilege Services
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID	Account lockout policy is set within Active Directory and can be set to lock the account for a specific duration as needed. Centrify enforces this policy on non- Windows systems. Since Centrify manages passwords on behalf of users there will be no invalid login attempts. Some use cases (e.g., "break glass") result in the password being revealed to an admin for interactive login. In this case, AD account logout policy can be set to lock the account for a specific duration.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session	**Centrify Zero Trust Privilege Services** provide a binary distribution of OpenSSH, configured to use the Centrify Kerberos libraries to ensure that a user will be able to gain single sign-on access to a remote host. The OpenSSH server can be configured to require that a user session times out after a specified period or inactivity, such as 15 minutes. After each timeout, it will challenge the user for authentication credentials.
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	**Centrify Zero Trust Privilege Services** support the listed factors in addition to, or in place of a password for authentication verification. Centrify supports MS Kerberos, X.509 certificates, RADIUS, and smart cards such as PIV and CAC. Policies can also be applied to require a second authentication factor consistently, or request one based upon policy-driven risk levels such as whether the user's mobile device is enrolled/trusted, whether the user is on the internal network, schedules and location. **Centrify Adaptive MFA for Privileged Access** can also be used to create a profile of user behavior and generate a risk score used to determine how MFA is used (or not) to assure the identity of the user.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components	Once systems are joined to Active Directory, all authentication will be encrypted on the wire and no passwords will traverse the network based on the Kerberos authentication process. Centrify stores passwords in a secure per-tenant store encrypted with AES256 bit symmetric keys or in a Gemalto® SafeNet™ Keystore appliance. These passwords are used over encrypted communications channels such as HTTPS (to the user), SSH (to *NIX servers) or RDP (to Windows servers).

#	Requirement	Centrify Zero Trust Privilege Services
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys	Centrify requires a user to properly authenticate before being allowed to perform such changes. Privileged shared account passwords are managed by Centrify, which will cycle these passwords on a scheduled basis and/or when a user checks a password back in after use.
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified.	Password policy is set within Active Directory and can be set for any length of password and require both mixed case as well as mixed alphanumeric construction. Centrify enables non-Windows systems to use much longer passwords than would otherwise be possible for the system to handle, since Active Directory is used to validate user passwords. **The Centrify Shared Account and Password Vault** manages shared privileged account passwords on behalf of the user. It sets these passwords automatically, based on configurable password complexity rules and password profiles. Based on role assignment, administrative users may be granted permission to rotate a password on-demand; the resulting password conforming to a specific password profile.
8.2.4	Change user passwords/passphrases at least once every 90 days	Active Directory's password policy can be set to expire and require reset on a time limit of 90 days or less. Centrify enforces this policy on non-Windows systems. Per 8.2.3 above, passwords can be automatically (or manually) rotated. Centrify's unique "multiplexed account" mechanism ensures no service downtime when rotating a password shared by for example multiple Windows services across multiple servers.
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used	Password policy is set within Active Directory and can be set to maintain password history and prevent the reuse of passwords. Centrify enforces this policy on non-Windows systems. When automatically rotating shared account passwords under Centrify management, the new password will be randomized within the constraints of the password policy, ensuring no repeat of prior passwords.

#	Requirement	Centrify Zero Trust Privilege Services
8.2.6	Set passwords/phrases for first- time use and upon reset to a unique value for each user, and change immediately after the first use	Centrify forces users to change their password upon initial login whenever the Active Directory account is configured to require the password to be changed at next login. This is normally set up on initial account creation as well as any time an administrator resets a user's forgotten password or locked account. Centrify can enforce such password procedures for users who login to the admin portal. Active Directory password policy governs this for privileged account passwords.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication	This requirement must be met by network access control systems prior to a user's access to a Windows, Linux or UNIX system. Once a user is authenticated properly to the remote network, access to the system is handled as if the user were on the local network. **Centrify Adaptive MFA for Privileged Access** supports "Authentication Profiles" that can be configured to require 1 or 2 user challenges. Each challenge can incorporate multiple second factors for the user to choose from, such as password, Centrify Mobile Authenticator, phone call, SMS text message, email confirmation code, user-defined security question, or an OATH OTP client. Risk-aware access policies can be implemented to protect critical IT infrastructure against attacks that exploit compromised privileged accounts. Whether initiating a privileged session or checking out a password, **Centrify Privilege Threat Analytics Service** determines the risk-level and either grants privileged access, prompts for an additional factor of authentication or blocks access entirely. Policies can be applied based on risk levels such as whether the user's mobile device is enrolled/trusted, whether the user is on the internal network, schedules and location.
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access	Centrify policies can enforce the use of multi-factor authentication for portal login. For resource account access, policies can require the use of MFA for both account password checkout as well as account session initiation. At the server/host level, policy can enforce the use of MFA during Windows, Linux, or UNIX server login. Once logged into a remote Linux, UNIX, or Windows server, Centrify policy can further enforce MFA during privilege elevation, selectively for specific applications.
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network	Centrify solutions have been designed specifically to accommodate remote login scenarios in a more secure fashion than traditional VPN-based methods. Remote sessions can be VPN-less via browser-based HTTPS connections or local SSH/RDP clients where the user is provided access to the specific target server instead of the broader network, sub-network, or jump-box. Since the user's computer is not network-attached, Centrify reduces exposure and obviates the potential risks of an infected computer spreading viruses or malware. Per 8.3.1, **Centrify MFA for Privileged Access** supports additional security at various levels of the remote user's session.

#	Requirement	Centrify Zero Trust Privilege Services
8.4	Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords Instructions to change passwords if there is any suspicion the password could be compromised.	Administrators need to inform users of the password policies and procedures. However, it is important to note that with Centrify, these policies and procedures are managed centrally in AD and enforced identically on Windows, Linux, and UNIX systems. **Centrify Zero Trust Privilege Services** are designed to assume responsibility for controlling and managing privileged shared account passwords. Thus, policies such as complexity and reuse of such passwords are handled automatically and not exposed to users. Generally, passwords are automatically rotated on a configured schedule. However, in suspicious circumstances, a password rotation can be forced. In this situation, **Centrify Zero Trust Privilege Services** control the complexity based on the password profile for that account/password. For additional protection, Centrify combines risk-level with role-based access controls, user context and multi-factor authentication to enable intelligent, automated and real-time decisions on whether to grant the user access, prompt for a second factor of authentication or block access.
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed • Shared user IDs do not exist for system administration and other critical functions Shared and generic user IDs are not used to administer any system components	**Centrify Zero Trust Privilege Services** create an environment whereby users log in with their own unique Active Directory account and explicitly request elevated privileges to run privileged commands. Centrify grants or denies these requests based upon a role-based access control mechanism. Ideally, shared and generic user IDs are disabled and can't be used to directly log in to the resource. This approach also ensures full accountability since privileged actions are now tied to a unique individual instead of an anonymous entity such as "root" or "administrator." Situations may occur where there is no choice but to enable shared accounts and permit direct login (such as upgrading an operating system). Centrify can take the password under management and automatically log the user in without revealing that password. It can then be cycled once the administrator's tasks are complete. Reports on Active Directory User IDs will allow the admin to see if there are any shared or generic accounts. If any shared or generic accounts do exist, the report will show what roles and privileges are associated. **Centrify Zero Trust Privilege Services** can also control which shared and generic user IDs are available for remote login by internal personnel and third parties such as partners and outsourced IT.

#	Requirement	Centrify Zero Trust Privilege Services
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Centrify supports several authentication mechanisms including Kerberos, X.509, PIV/CAC cards, and derived credentials. Centrify associates unique login credentials to a person based on their unique Active Directory entry. Authentication and access control mechanisms ensure that only authorized users can gain access to the resources they're entitled to use via such means.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods • Only database administrators have the ability to directly access or query databases Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).	Centrify provides configuration tools and plugins as needed to integrate the authentication of Oracle, DB2, Sybase and Informix databases into Active Directory to enable centralized account and password policy enforcement.

#	Requirement	Centrify Zero Trust Privilege Services
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1	Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user	**Centrify Zero Trust Privilege Services** establish a valid user context for the UNIX account, which is linked directly to a unique Active Directory account to ensure that all audit trails can be traced back to an individual person. Centrify enforces a model of least privilege whereby each user logs in with a personal, unambiguous ID. All activities are therefore tied back to the user, ensuring individual accountability. Centrify users log in with their own individual ID, so activities are fully accountable. Note that in a vault-only architecture, where session recording is only performed on a single proxy tied to the password vault, administrative activity will not be captured if the user bypasses the vault and goes directly to the server. **The Centrify Audit and Monitoring Service** solves this with the ability to capture sessions at the proxy and/or the host level for full accountability. The Centrify Audit and Monitoring Service also monitors process calls from the system kernel, which thwarts spoofing techniques and enables deep forensic analysis for corrective action and compliance. Running commands as a different user, within a script or leveraging command aliases are all accurately detected, audited and attributed back to the actual individual. For example, after an "su root", all activities will be associated with the original User ID.
10.2	Implement automated audit trails for all system components to reconstruct the following events:	See below for details on how **Centrify Zero Trust Privilege Services** meet these requirements.
10.2.1	All individual user accesses to cardholder data	Centrify enables tracking of all user authentication and account management operations through the logs maintained on the Active Directory domain controller performing the action. The domain controllers will log all login attempts, both successful as well as invalid. **The Centrify Audit and Monitoring Service** creates and centrally stores a log of all user action taken on the system for Active Directory users as well as local accounts. The log contains all actions taken regardless of the privilege level of the user, including any user access of the audit trails or logs and system level objects. Since the audit logs are stored within a central system that is not located on the audited system, security is enhanced with a second machine that also enforces access controls on all database privileged access. **The Centrify Audit and Monitoring Service** uniquely monitors at both the shell and process levels, attributing all activity to the individual versus a shared account. For privileged activities, the **Centrify Audit and Monitoring Service** can record sessions for detailed review of all activities on the screen. Centrify will audit and record session activity for all sessions initiated through the jump box (i.e., break-glass is not audited). It will also audit activities performed at the portal level – login, password checkout, request to remotely login, etc.

#	Requirement	Centrify Zero Trust Privilege Services
10.2.2	All actions taken by any individual with root or administrative privileges	To enable tighter controls around privileged operations, Centrify provides a Group Policy to enable centralized management of sudo permissions to ensure that the appropriate permissions are applied to local accounts in a consistent manner across the computers where this privilege should be granted. Centrify extends this functionality to define a set of roles that will be granted specific access and privileged command rights. These roles are defined on Active Directory, enabling both AD users and AD groups to be assigned to the role, simplifying ongoing management. Centrify also provides a mechanism to control the root account password policy through Active Directory to further protect those accounts that would otherwise be able to gain unbridled access to a non-Windows system. Centrify also provides a mechanism to control the root account password policy through Active Directory to further protect those accounts that would otherwise be able to gain unbridled access to a non-Windows system. **The Centrify Audit and Monitoring Service** creates and centrally stores a log of all user action taken on the system for both Active Directory users and local accounts. The log contains all actions taken, regardless of the privilege level of the user, including any user access of the audit trails or logs and system level objects. Since the audit logs are stored within a central system that is not located on the audited system, security is enhanced with a second machine that also enforces access controls on all database privileged access. For privileged activities, the **Centrify Audit and Monitoring Service** records sessions for detailed and indexed review of all activities on the screen. Centrify audits and records session activity for all sessions initiated through the jump box (i.e., break glass is not audited). It will also audit activities performed at the portal level — login, password checkout, request to remotely login, etc.
10.2.3	Access to all audit trails	As with files or databases containing audit information, access to audit trails can be protected like any other system resource using least-privilege access, role-based access controls, and privilege elevation. Within the **Centrify Zero Trust Privilege Services**' administrative UIs, access to audit trail data through the query engine and built-in reports can be governed by roles, logging all auditing activity.

#	Requirement	Centrify Zero Trust Privilege Services
10.2.4	Invalid logical access attempts	Active Directory and Linux will log invalid authentication attempts. Active Directory logs invalid workstation logins or Kerberos ticket requests to unauthorized systems. Linux logs invalid login attempts performed interactively. **The Centrify Audit and Monitoring Service** audits activities performed at the portal level — login, password checkout and requests to remotely login. **The Centrify Audit and Monitoring Service** also identifies suspicious changes to configurations and files such as SSH keys being stored locally on servers used as a back-door to bypass the password vault.
10.2.5	Use of and changes to identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges — and all changes, additions, or deletions to accounts with root or administrative privileges	Centrify defines a set of roles that will be granted specific access and privileged command rights. These roles are defined in Active Directory, enabling both Active Directory users and groups to be assigned to the role, simplifying ongoing management. These tools also serve to produce an audit trail of all privileged operations, since sudo will log all command execution where the simpler "su" command does not provide this level of visibility, nor does allowing a user to login as the root account. In addition, **The Centrify Audit and Monitoring Service** detects activity such as running commands as a different user, within a script or leveraging command aliases and attributes them back to the actual individual. Centrify also provides a mechanism to control the root account password policy through Active Directory to further protect those accounts that would otherwise be able to gain unbridled access to a non-Windows system. Centrify creates and centrally stores a log of all user action taken on the system for both Active Directory users as well as local accounts. The log contains all actions taken regardless of the privilege level of the user, including any user access of the audit trails or logs and system level objects. Since the audit logs are stored within a central system that is not located on the audited system, security is enhanced with a second machine that also enforces access controls on all database privileged access. For privileged activities, Centrify can record sessions for detailed and indexed review of all activities on the screen.
10.2.6	Initialization, stopping, or pausing of the audit logs	**The Centrify Audit and Monitoring Service** monitors its own audit logging via heartbeat to the central audit log database.

#	Requirement	Centrify Zero Trust Privilege Services
10.2.7	Creation and deletion of system-level objects	Since Centrify advocates a least privilege model, whereby unique identities are used to login versus shared accounts, these log entries map back to the actual user instead of an anonymous user. All user activities that are logged by Centrify include the identity of the user performing actions such as system-level operations on objects. Centrify file change and command execution monitoring identifies changes to configurations and critical files in real time, triggering security alerts within an organization's SIEM system to warn of the creation of a backdoor to bypass the password vault. Monitoring process calls from the system kernel prevents spoofing techniques and enables deep forensic analysis.
10.3	Record at least the following audit trail entries for all system components for each event: User identification; type of event; date and time; success or failure indication; origination of event; identity or name of affected data, system, component, or resource	**Centrify Zero Trust Privilege Services** maintain audit trails (e.g., syslog, Windows Event Log, and its own audit database) as well as session recordings of privileged activities. Centrify captures all the data identified in 10.3.1 through 10.3.6.
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time	Centrify automatically configures and enforces the Time Sync Policy defined within Active Directory Group Policy on all UNIX and Linux systems that are joined to Active Directory. This time sync will be performed with the Active Directory domain controller infrastructure, which should be configured for time sync with a stratum 1 clock.
10.5	Secure audit trails so that they cannot be altered	**Centrify Zero Trust Privilege Services** have been architected to prevent unauthorized viewing or manipulation of the user session logs. This is accomplished by the audit daemon as it securely transmits the audit log to a centralized collector which will store the data in an SQL Server repository under tight access control policies. The audit logs are typically not stored locally, unless the network connectivity to the collector is down, at which time it will cache locally and spool off to the collector when network connectivity is restored. **The Centrify Audit and Monitoring Service** only allows authorized auditors to view the user sessions once logged in using their Active Directory credentials to the workstation running the console. This is designed to control which personnel have access to the centralized logs.

#	Requirement	Centrify Zero Trust Privilege Services
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity	Centrify stores the audit data in a plain text, non-proprietary format so that other tools such as SQL Reporting Services can be used to analyze the data and generate alerts as needed.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Standard data backup and restore procedures can be used to manage the log data that Centrify stores within the SQL Server repository to enable a backup policy that complies with this requirement.
Requirement 11: Regularly test security systems and processes		
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date	While **Centrify Zero Trust Privilege Services** are not specifically designed as an intrusion prevention system, it can be configured as described above to only allow specific trusted systems to communicate, thus preventing intruders from accessing PCI systems. **Centrify Zero Trust Privilege Services via its isolation and encryption capabilities** leverage Group Policy to manage the local IPsec and firewall security policies as defined within Active Directory to ensure that these policies are kept up-to-date.
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Centrify has unique visibility of users and their entitlements ("who has access to what") as well as their activities ("who did what"). It can pre-correlate this data and make it available to a customer's existing Security Information and Event Management (SIEM) solution to be used as part of a detective change-detection mechanism.

#	Requirement	Centrify Zero Trust Privilege Services
Requirement 12: Maintain a policy that addresses information security for all personnel		
12	Maintain a policy that addresses information security for all personnel	Centrify leverages Active Directory to centrally define and manage user identities, resources, and policies consistently across Windows and non-Windows platforms. It also logs and records privileged session activities. As such, this is an important feed into a customer's information security and risk assessment program.
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk	Centrify helps risk assessment and security spot checks with the option to selectively record session activity associated only with the execution of privileged commands, instead of the entire login session. **The Centrify Audit and Monitoring Service** includes event-based logging and auditing as well as visual session recording with video playback. Session transcription isolates specific activities and commends entered to help companies streamline their risk assessment and forensic investigations, allowing them to quickly focus on privileged activities where policy violations have been attempted.

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 use cases. 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

www.centrify.com