WHITE PAPER • MAY 2017

ca technologies

The Payment Card Industry Data Security Standard and CA Privileged Access Management

Table of Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) was first introduced in 2004 to increase controls over credit card holder data and to reduce the chances of credit card fraud. Validation is required annually and over the years, it has evolved with new revisions periodically. The latest one, version 3.2 came into force in April 2016. Until the end of January 2018, PCI DSS and Payment Application Data Security Standards (PA-DSS) are considered best practice to implement, and starting February 1, 2018, are considered a requirement.

SECTION 1

Key requirements of PCI DSS 3.2

Here are the key requirements of PCI DSS:

PCI Data Security Standard - High Level Overview

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

At a high level, these requirements address a broad range of security measures. However, as part of this document, we'll examine those requirements that are relevant to managing privileged users.

Why is managing privileged access important?

As they say, you're only as strong as the weakest link in the chain. Often, the weakest link is the one that is out of plain sight. Privileged identities are often the least visible, until an uncomfortable truth is revealed in the form of a breach or failed compliance. Here are a few key aspects of privileged access:

Omnipresent. Any organization has users who have elevated access to specific applications. The most visible are users with administrative privileges. However, with changes in software development and with digital transformation, the nature of identities with privileged access is significantly changing. With organizations moving to virtual environments and the cloud for infrastructure, platform and applications, users within departments assumed additional privileges. Adoption of agile methodologies has led to more application-to-application (A2A) interactions. The list goes on, and as one can imagine, it will only grow bigger.

Potent. As should be obvious, privileged access to any application or infrastructure comes with significant responsibilities. Such users or identities have access to sensitive data and any malicious access or accidental mishaps can inflict significant damage and cause reputational risk. In each of the previously stated instances, if the user deletes data, accidentally or intentionally, from a mission-critical server or changes the configuration on a production server without oversight, there is real business impact and cause for concern.

Preferred targets. Given the criticality of access that privileged users and identities have, they're highly sought after by any party trying to cause harm. Very often, they're the target of attacks, and if an organization doesn't maintain the right security posture, it's very likely to be impacted by an attack.

For the reasons mentioned above, it's very important to manage privileged user access. Additionally, depending on the industry you're in, such access may also be mandated by regulations either directly or indirectly. PCI DSS has such mandates in place. In fact, the changes introduced in version 3.2 have many direct and indirect implications for how privileged access is managed. In the rest of this document, we'll review specific requirements of PCI DSS 3.2 as they apply to privileged access.

Privileged access management and PCI DSS 3.2

Several sections of the PCI DSS standard were enhanced in version 3.2 to reflect the changing business reality. Some of these changes apply to how privileged access is managed. The following table details the requirements defined by PCI DSS and how they're relevant to privileged access management.

Requirement	Changes in version 3.2	Impact on privileged access management
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	Multiple sections were changed to indicate intent; 1.3.3 was removed.	This requirement mandates the need for managing groups and roles of users who have access to configuration of firewalls. Additionally, this requirement implicitly requires privileged access management to: • Ensure that no outbound traffic leaves the cardholder data environment. • Manage and monitor all changes to configuration files.
Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters.	There were mostly just clarifications issued as part of this version.	This section has wide-ranging implications on privileged identities and access. Most software and hardware today ship with default passwords. Additionally, the policies for these passwords vary significantly. To start with, one needs to identify all assets that come under the purview of the requirements of the standards. These assets may be on premises, virtual or on multiple cloud environments. Not only should the privileged access management solution help in discovery of these assets but it should help in setting policies for the passwords, record sessions and help control access to these assets across all boundaries (cloud, virtual and on-premises). Finally, controlled access needs to be granular enough to provide that changes to any security configuration on any of these systems are secured and monitored.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.	No changes.	There are multiple ways of protecting against malware. While anti-virus software is explicitly called in the requirement, as a best practice, organizations should consider all means of protecting against malware. Privileged access management provides ways in which organizations can protect against malware. For example, for those systems that have anti-virus programs, administrative access for upgrades and maintenance should be controlled sufficiently. For other systems that contain cardholder data, organizations can implement isolation strategies, categorize applications and infrastructure and control access to these systems. Additionally, users can be restricted in the commands they execute. Further, with advances in machine learning and user behavior analytics, we can proactively mitigate any suspicious activity, even in the case of an account takeover. This is even more critical when one considers the scale and scope of challenges that organizations face, rendering manual techniques untenable. Finally, privileged access management solutions also enable us to monitor and record any activity using techniques such as keylogging and screen recordings.
Requirement 6: Develop and maintain secure systems and applications.	Changes are limited to specific sections and are for guidance.	This section deals with the overall security best practices to be followed when developing and maintaining software and systems that access cardholder data. The guidance for this requirement covers aspects such as: • Ensuring that the most recent patches are applied to the systems, • Developing software which provides that proper security procedures are followed • Following the segregation between production and non-production applications and servers Privileged access management solutions can significantly help address this requirement. For example, when maintaining systems and applying patches etc., organizations need to ensure that there are sufficient control procedures in place with the right level of authentication and oversight. For example, while an administrative user may be permitted to run a command to patch a server, additional controls and approvals may need to be enforced if it is production system. Applications may programmatically access cardholder data and need credentials to do so. Finally, this requirement covers the need for segregation of duties of users accessing various environments (developer, test and production environments). Privileged access management solutions can help in managing these credentials rather than embedding them within the applications. Segregation of duties requirements can be met by integration between privileged access management solutions and automation tools.

Requirement 7: Restrict access to cardholder data by business need to know.	Changes made to guidance and testing to cover multiple systems.	This requirement covers the need for various users' access to any application or system that contains sensitive data to be controlled based on roles, business need and by means of least privileges. Such access should be logged and auditable. Privileged access management solutions help address this requirement by means of managing users in groups and by defining what users are permitted to do on a specific application or a group of applications. Further, by leveraging integrations with other solutions, privileged access management solutions can provide for workflow-based provisioning and deprovisioning of access to various applications and systems. Eventually, this access can also be recorded, logged and audited.
Requirement 8: Identify and authenticate access to system components.	Perhaps the most significant changes in the current version occurred in this requirement. There is now a requirement for all non-web-based and remote access for sensitive data to be protected by multifactor authentication (MFA). Additionally, the earlier requirement of two-factor authentication has been extended to include multifactor authentication.	This requirement is probably the one with far-reaching impact on privileged accounts. All such accounts, whether accessed directly or indirectly and when accessed remotely all need to be protected with MFA. All user access must be logged and must be traceable. The requirement mandates unique identity for all users who access such systems. Users' access must be configured based on least privilege and all actions must be auditable. Proper user lifecycle management (provisioning, deprovisioning and modification) must be put in place to provide for creation, deletion and modification of users and their access. Any user information including credentials must be managed using strong cryptography. Any password or passphrase should adhere to specific policies for strength and rotation. The requirement also mandates that shared credentials should not be used for specific applications. Proper controls are required to provide that commands run on databases that contain cardholder data are limited based on the role and business need (only database administrators), and all other access is rejected.
Requirement 10: Track and monitor all access to network resources and cardholder data.	An additional requirement was added necessitating the timely detection and reporting of any security failures in service provider environments.	This requirement mandates the need to maintain complete audit trails of all users, their access and any changes that may occur in any rules, configurations and access controls of specific fields across all resources on the network.

Requirement 11: Regularly test security systems and processes.	Most changes here were related to penetration testing requirements that do not directly impact privileged access management.	One of the mandates issued as part of this requirement is the need to implement intrusion detection systems to determine risks. However, with changes in the computing landscape, it's now possible to use machine-learning techniques to proactively mitigate threats based on user behavior.
Requirement 12: Maintain a policy that addresses information security for all personnel.	Changes to this requirement in the latest version are mostly in clarifications and testing procedures.	Any privileged access management solution should support policies that govern access and allow privileged users to create, modify and delete security policies for all personnel. All actions should be auditable and traceable to the specific user that conducted that transaction.

SECTION 2

CA Privileged Access Manager and Support for Requirements of PCI DSS 3.2

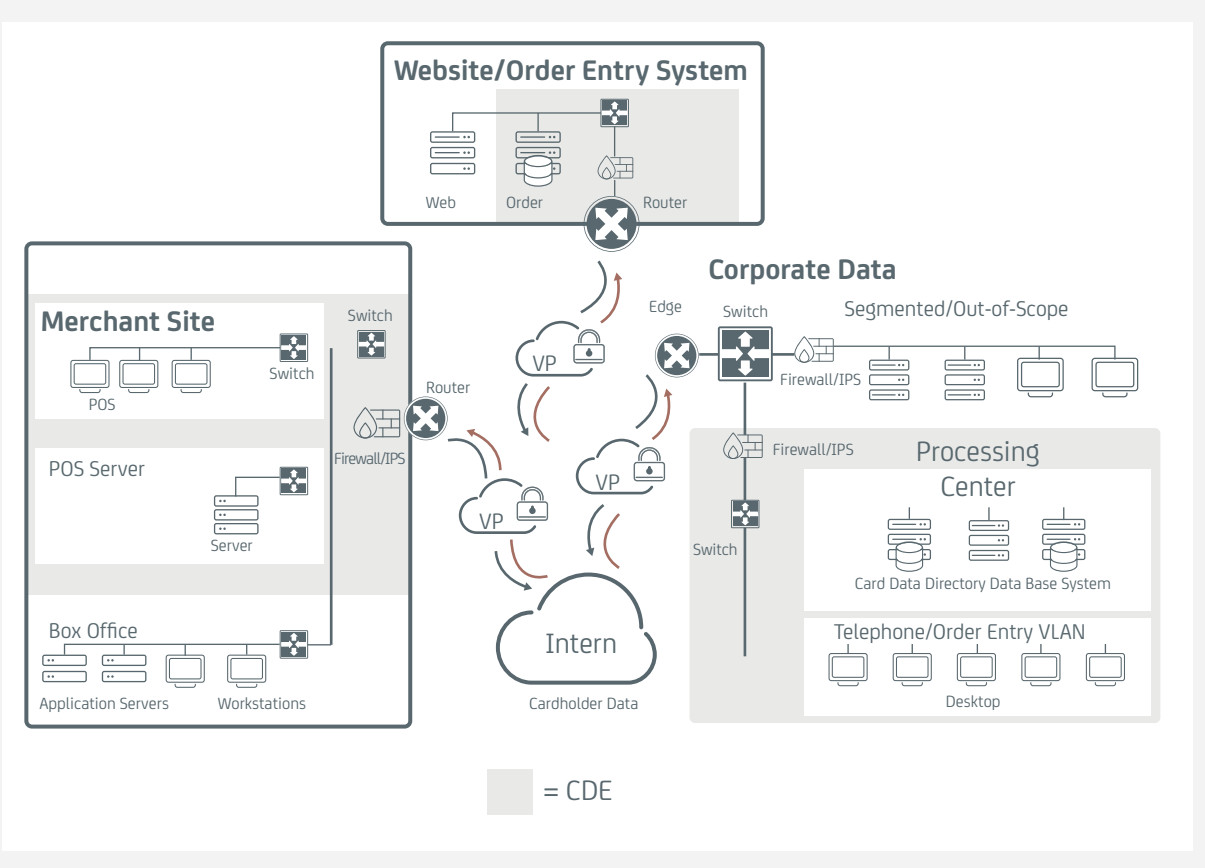
Interrupting the breach kill chain

The basic concept of a kill chain is that an attacker follows a repetitive pattern of gaining access to a system (or expanding that access), then elevating privileges. Those privileges are then used to move horizontally or vertically and gain access to another system or expand existing access, then elevate privileges again and continue this chain of exploitation until the final target is reached. If this chain of exploitation can be broken at any point in the cycle, the attack can be stopped before it reaches its ultimate target.

CA Privileged Access Manager (CA PAM) provides the capabilities that help interrupt the kill chain. For example, CA PAM supports multifactor authentication for privileged accounts, making them much harder to compromise because an attacker needs to compromise multiple credentials for a single account. Also, the use of least privilege when it comes to which commands each privileged account can issue on each cardholder data environment (CDE) component, reduces access to sensitive information, making it more difficult for an attacker to gain unauthorized access to data of interest.

Another way CA PAM helps interrupt the kill chain is via its support of network segmentation. This restricts which subnets a particular privileged account can access and which systems on each subnet can be administrated. Network segmentation helps limit the lateral spread of attacks from one system to another and restricts attacker visibility into an organization's network. Similarly, CA PAM offers a socket filter agent (SFA), which prevents an administrator from opening an unauthorized network connection to another system, such as attempting to SSH or telnet to a host not authorized by CA PAM policy.

FIGURE 1.
Segmentation for PCI DSS compliance.



CA's privileged access management solution helps organizations address PCI DSS 3.2 requirements. Various features of the solution are described in this section. Additionally, when combined with other integrated CA Security solutions, organizations can adopt a robust, scalable and full-features solution to address their PCI DSS needs. The table below discusses in more detail how CA PAM can help address the latest PCI DSS requirements.

Requirement	Changes in version 3.2
1.1: Establish and implement firewall and router configuration standards.	CA's privileged access management solution provides the ability for only specific sets of privileged users to establish, implement and manage firewall and router configuration.
1.1.5: Description of groups, roles, and responsibilities for management of network components.	CA's solution provides the ability to create groups of users, assign specific roles and privileges to those users to provide for segregation of duties and appropriate responsibility for management of network components, servers and applications. CA also supports management of virtual network environments such as VMWare NSX, providing a comprehensive, scalable solution. When integrated with CA identity management and governance solutions, the process of assigning users to groups and roles can be automated.

1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	While this requirement focuses on the need to monitor inbound and outbound traffic, with CA Privileged Access Manager Server Control, organizations can provide that specific commands are not permitted on a set of servers, thereby ensuring that data does not leave an organization's network.
2: Do not use vendor-supplied defaults for system passwords and other security parameters.	CA PAM supports the changing of default passwords and other security parameters, such as the permitted network access methods for administrators.
2.1: Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	CA PAM vaults and manages administrative passwords/ credentials. This includes forcing the change of default passwords.
2.3: Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	CA PAM enforces access policies, providing that individuals are only able to access systems via approved (encrypted) protocols. Because all administrative passwords and credentials are maintained in an encrypted vault, an administrator is not able to circumvent these access policies. CA PAM provides an SSL VPN to protect administrative traffic from eavesdropping and manipulation, and access to the CA PAM console itself is likewise protected with TLS (HTTPS).
5.1: Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	CA privileged access management permits specific users to manage the installation and upgrade of specific applications on a set of systems. This can be based on groups or roles of those administrative users. Systems and servers can also be whitelisted or blacklisted to help ensure that any malware that has made its way does not spread. Using CA Threat Analytics for PAM, organizations can also detect what may be suspicious activity and launch mitigation strategies.
6: Develop and maintain secure systems and applications.	CA PAM helps organizations eliminate A2A passwords from scripts, code and configuration files that are part of cardholder data processing systems, removing an important vulnerability where administrative passwords are stored in plaintext and can be accessed by application developers and testers. While this vulnerability is not specifically called out in the requirements, it remains a very high-risk issue, particularly for homegrown systems, applications and scripts that are integrated with cardholder databases—for example, for reporting and upstream or downstream transaction purposes.

6.3: Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging). • Based on industry standards and/or best practices. Incorporating information security throughout the software development life cycle.	See requirement 6.3.1.
6.3.1: Remove development, test and/or custom application accounts, user IDs and passwords before applications become active or are released to customers.	Leveraging CA PAM, organizations can move passwords from application code to the encrypted vault and use CA PAM APIs to provide that only specifically authorized calling applications can request a password. The password remains encrypted from vault to target system, across the network and in memory. Further, via integration with CA identity management and governance solutions, only those users who are permitted to manage provisioning and deprovisioning of application accounts, users and credentials can do so.
6.4: Follow change control processes and procedures for all changes to system components. The processes must include the following:	See requirement 6.3.1.
6.4.2: Separation of duties between development/test and production environments.	CA PAM enforces role-based access control for the privileged accounts on systems used in development, test and production. When integrated with CA identity management and governance soltuions, CA PAM can provide the right level of user access based on roles, privileges and segregation of duties polices.
7: Restrict access to cardholder data by business need to know.	CA PAM implements a comprehensive set of controls for restricting access to system components and cardholder data. The controls help organizations implement a zero-trust model that extends the concepts of least privilege to "no privileges without specific authorization." Our zero-trust model enforces fine-grained access control, monitoring and recording of all privileged user sessions. With privileged governance (integration between CA PAM and CA identity management and governance solutions), it's possible to provide that the entire user lifecycle of creation, read, update and delete operations for all systems be controlled. This provides for segregation of duties and simplifies compliance reporting.

7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access.	CA PAM implements the least privilege principle in many ways. It enforces fine-grained access control on privileged users, who must be explicitly granted access to servers, network devices and other system components. The solution also uses command filtering (whitelists and blacklists) to limit which commands authorized users can run. With privileged governance (CA PAM and CA identity management and governance solutions), users can be provided access to such data through a complete approval process, any changes to privileges can be governed and all access privileges can be reported and certified for regulatory purposes.
7.1.1: Define access needs for each role, including: • System components and data resources that each role needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Because CA PAM fully supports role-based access control, it provides a mechanism well-suited for defining access needs for each administrative role (e.g., database, network or system administrators). This includes restricting which system components and data resources within those system components each administrative role may access.
7.1.2: Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	This is at the heart of CA PAM capabilities. Each privileged user ID or groups of privileged user IDs can have access restricted to only those commands necessary for each authorized system component.
7.1.3: Assign access based on individual personnel's job classification and function.	CA PAM enforces policies applied to individuals or groups. Group and role definitions can be established in CA PAM directly or by leveraging the solution's integration, and using group and role definitions that already exist in enterprise directories. Further, with the integration with CA identity management and governance solutions, the process of provisioning and deprovisioning access to users based on business roles, groups or locations makes the process easier to manage. Wrongfully granted privileges to administrative users can be remediated.
7.1.4: Require documented approval by authorized parties specifying required privileges.	CA PAM can enforce a dual authorization that requires (and logs) approval by an authorized individual before a password is released.
7.2: Establish an access control system for systems components 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:	CA PAM separates authentication from authorization. Users log into CA PAM using strong (multifactor) authentication methods. From there, they are provided with a list of components they have been explicitly authorized to access. Users do not have visibility or access to non-authorized components.
7.2.1: Coverage of all system components.	As defined by PCI DSS, system components include servers, network devices and applications. CA PAM provides coverage for all the PCI DSS-defined components, including off-the-shelf applications.

7.2.2: Assignment of privileges to individuals based on job classification and function.	CA PAM denies all access unless an individual is explicitly granted access through an individual or group policy.
7.2.3: Default "deny-all" setting.	CA PAM denies all access unless an individual is explicitly granted access through an individual or group policy.
8: Identify and authenticate access to system Components.	CA PAM requires a unique user login to identify each user, and the solution supports many authentication technologies. It's also important to ensure that any access to shared accounts can be traced back to the actual user. In the case of any automated access to system components, it may be required to know which user's action initiated the access. CA PAM offers solutions to these accesses. To minimize risky access to these system components, CA Threat Analytics for PAM offers a way to flag access for further mitigation.
8.1: Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	CA PAM supports the enforcement of policies for managing the identities of all privileged accounts for all system components. See 8.1.1 through 8.1.8 below for more details.
8.1.1: Assign all users a unique ID before allowing them to access system components or cardholder data	CA PAM requires a unique user login to the CA PAM platform, and then establishes a privileged session to an authorized system component. In this configuration, organizations can leverage "shared accounts" for infrastructure components (e.g., root) for ease of management while also tracking every privileged session to a specific individual (not just an IP address).
8.1.2: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	CA PAM enforces separation of duties, so only specifically authorized administrative users can make changes to its privileged IDs and other credentials. These special CA PAM administrative users must use strong multifactor authentication methods, and each of these sessions is logged and recorded. This can be further enhanced by the integration with CA identity management and governance solutions.
8.1.3: Immediately revoke access for any terminated users.	CA PAM enables organizations to immediately terminate all access to all system components for privileged users who have been terminated.
8.1.4: Remove/disable inactive user accounts at least every 90 days.	CA PAM supports automatically deactivating CA PAM accounts that have not been used for a set period.

8.1.5: Manage IDs used by vendors 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.	CA PAM has the same capabilities for managing privileged vendor IDs as any other privileged ID. This includes enforcing time-limited access for vendors. Additionally, the solution monitors and records each privileged session and can send alerts and automatically terminate access based on attempted policy violations.
8.1.6: Limit repeated access attempts by locking out the user ID after not more than six attempts.	CA PAM enforces failed attempt policies, including locking out a CA PAM account after an administrator-defined number of failed access attempts.
8.1.7: Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	CA PAM can enforce options such as locking out an account until an authorized administrator re-enables it.
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.	CA PAM can be configured with a session timeout, which is set to default by 10 minutes.
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.	CA PAM supports integration with numerous authentication methods including strong, multifactor authentication systems. The solution passes an authentication request to the chosen authentication system (e.g., AD, RADIUS, smart card). Once the individual has been successfully authenticated, CA PAM provides the user with a list of explicitly authorized resources they can access and the access methods they can use, based on individual or group policies in CA PAM. This enables organizations to separate authentication from authorization.
8.2.1: Using strong cryptography, render all authentication credential (such as passwords/phrases) unreadable during transmission and storage on all system components.	CA PAM stores passwords and other authentication credentials in an encrypted vault. The solution uses FIPS 140-2 security kernels for all cryptographic operations. Integration with hardware security modules (HSMs) is available to achieve higher levels of FIPS 140-2 compliance. Passwords and other credentials are transmitted over secure/encrypted channels.
8.2.2: Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	CA PAM can be configured to require successful authentication before enabling a password reset, generating new cryptographic keys, etc.
8.2.3: Passwords/phrases must meet the following: Require a minimum length of at least seven characters. Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	CA PAM enforces industry-standard password length and strength/composition policies, including minimum password length and the use of different types of characters.

8.2.4: Change user passwords/passphrases at least every 90 days.	CA Privileged Access Manager enforces password changes on any time interval. The system's password management capability performs the change automatically based on policies established in the system.
8.2.5: Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	CA PAM enforces industry-standard, fully configurable password reuse policies, which include administrator-determined settings for how many iterations are required before a password can be reused, and how many days a password must be used before it can be changed again.
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.	CA PAM implements a comprehensive set of password policies including password composition, reuse and aging. These policies support one-time use, and can even be configured to automatically set a new password after each use. Another option is to allow a password to be checked out and automatically set a short time limit for this password to be viable.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	CA Privileged Access Manager supports numerous multi-factor authentication methods and supports RADIUS and X.509 certificates and smart cards. CA Privileged Access Manager can enforce strong multi-factor authentication before enabling a privileged user's access to authorized resources. Further with integration with CA's industry leading Advanced Authentication capabilities, organizations can initiate multi-factor authentication. With Threat Analytics of PAM, when the behavior of privileged users defies normal behavior, such sessions can be terminated. Multi-factor authentication can be forced at next login.
8.3.1: Incorporate multifactor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance).	CA PAM supports numerous multifactor authentication methods and supports RADIUS and X.509 certificates and smart cards. CA PAM can enforce strong multifactor authentication before enabling a privileged user's access to authorized resources. Further, integration with CA's industry-leading advanced authentication capabilities, organizations can initiate multifactor authentication. With CA Threat Analytics for PAM, when the behavior of privileged users defies normal behavior, such sessions can be terminated. Multifactor authentication can be forced at next login.

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.	In a traditional configuration, the issue with shared accounts is that there is no way to tell who did what. If everyone logs in as root or admin, then each privileged user is effectively anonymous. But shared, generic or group accounts significantly simplify the configuration and management of system components, especially in large networks. With CA PAM, you can have the best of both worlds—fully attributed (and verifiable) use of shared accounts. Organizations can continue to configure servers, network devices and other components using shared accounts, but still have a specific and verifiable record of exactly which individual was logged into the shared account and exactly what they did. The passwords to these shared accounts are stored in the CA PAM vault, so users are forced to log into CA PAM before they are granted access to a shared account. Once users are logged into the shared account, CA PAM monitors and records everything so any privileged user activity performed using a shared account can be traced back to the specific user.
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.	CA PAM supports the use of many authentication mechanisms, including security tokens, smart cards and digital certificates. Each of these mechanisms can be assigned to an individual, unique ID, with additional authentication mechanisms used in conjunction to help ensure that only the authorized person can gain access through the security token, smart card or digital certificate.
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).	CA PAM restricts direct access to cardholder databases to only authorized administrators. The solution also provides that application accounts can only be used by applications.
10.1: Implement audit trails to link all access to system components to each individual user.	CA PAM links all privileged access to a specific user. It supports strong, multifactor authentication to help ensure that only authorized individuals are able to access system components using privileged accounts, and so that each privileged session can be specifically attributed to the authorized user.
10.2: Implement automated audit trails for all system components to reconstruct the following events:	Every action that a privileged user takes on a system component—server, database, network device, application, etc.— is recorded by CA PAM in a tamper-evident log that only specifically authorized individuals can access and review. See 10.2.1 through 10.2.7 below for more details.

10.2.1: All individual user accesses to cardholder data.	All administrator accesses to cardholder databases, such as by authorized database administrators, are monitored and recorded by CA PAM.
10.2.2: All actions taken by any individual with root or administrative privileges.	CA PAM monitors and records all privileged activity. Even if organizations are using shared administrative accounts, CA PAM can specifically attribute each action taken to a unique user.
10.2.3: Access to all audit trails.	CA PAM provides separation of duties so that only specially authorized users can review CA PAM log files and recordings. Every time an authorized user reviews a log, that fact is also logged—and can be recorded.
10.2.4: Invalid logical access attempts.	CA PAM tracks all invalid logical access attempts originating through the CA PAM platform. First, only authorized users can gain access to CA PAM, and once they have, they're only provided access to systems for which they are explicitly authorized. After accessing an authorized system, CA PAM can also prevent attempts to use an authorized system to gain access to an unauthorized system (leapfrogging or RDP hopping). CA PAM does not log failed login attempts performed outside of the platform—e.g., attempts to directly connect and log into a server. But since all passwords/ credentials are stored in the CA PAM vault and are not known by users, individuals have no way to log into these systems other than through the CA PAM platform.
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.	CA PAM logs all identification and authentication activities for privileged accounts, including all changes involving these accounts and all use of these accounts.
10.2.6: Initialization, stopping, or pausing of the audit logs.	CA PAM does not have a log entry to show that logging was initialized; rather, by default, the solution constantly generates logs.
10.2.7: Creation and deletion of system-level objects.	In CA Privileged Access Manager, authorized administrators can create and delete target servers, accounts, passwords, groups, users, etc.
10.3: Record at least the following audit trail entries for all system components for each event:	CA PAM records a full-fledged audit trail for privileged access to all system components. See the responses below for 10.3.1 through 10.3.6 for more details.

10.3.1: User identification.	Users are authenticated via strong, multifactor methods so that the unique user is captured in the logs and recordings that CA PAM maintains.
10.3.2: Type of event.	CA PAM syslog events are categorized including login/logout attempts, policy violation attempts, remote session establishment, etc.
10.3.3: Date and time.	Date and time are captured as part of the syslog and session recording streams.
10.3.4: Success or failure indication.	For each event where success or failure is relevant, such as login/logout attempts, CA PAM logs success or failure.
10.3.5: Origination of event.	CA PAM captures the unique user identity and source IP address used to access the solution for each event.
10.3.6: Identity or name of affected data, system component, or resource.	For events that affect a system component, resource, etc., the identity of the affected target (e.g., hostname) and the user accessing the system are captured.
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.	CA PAM supports industry-standard time- synchronization technology—Network Time Protocol (NTP).
10.4.1: Critical systems have the correct and consistent time.	CA PAM performs time synchronizations using NTP to provide that it has correct and consistent timestamps for its audit logs and recordings.
10.4.2: Time data is protected.	CA PAM can be configured to use authenticated NTP, which provides a higher level of integrity than basic NTP.
10.4.3: Time settings are received from industry-accepted time sources.	Two default time servers are specified, and authorized CA PAM administrators can augment and/or change these.
10.5: Secure audit trails so they cannot be altered.	CA PAM logs and recordings are protected from unauthorized access and modification, and any changes that do occur are detected.
10.5.1: Limit viewing of audit trails to those with a job-related need.	CA PAM logs and recordings are only accessible to explicitly authorized personnel, following the principles of least privilege and role-based access control.

10.5.2: Protect audit trail files from unauthorized modifications.	All CA PAM logs and recordings are tamper evident using cryptographic hashing techniques. CA PAM will notify that a file has been tampered with.
10.5.3: Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	CA PAM provides syslog forwarding, which allows backup of all CA PAM logs to centralized syslog servers, write-once media and other forms of log storage and archival.
10.5.5: Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	CA PAM logs and recordings are tamper-evident using cryptographic hashing techniques. Any modification of an existing log or recording, other than standard addition of new data, will be detected.
10.6 (including 10.6.1 to 10.6.3): Review logs and security events for all system components to identify anomalies or suspicious activity.	CA Threat Analytics for PAM provides a robust machine-learning based, user-behavior-analytics (UBA) solution. This solution works along with SIEM solutions and other enterprise logging solutions, and can be used to determine risk associated with user-based activity. Any risk determined can be mitigated using a variety of techniques.
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).	Because CA PAM uses syslog, an audit trail can be kept on a syslog server for as long as deemed necessary. This frees storage space on the local CA PAM system while keeping the log data immediately available for analysis. The local CA PAM system can retain logs for as long as four months.
12: Maintain a policy that addresses information security for all personnel.	CA PAM enables organizations to capture and enforce privileged user policies that protect cardholder data. The solution makes it very easy to prove that required controls are in place for each system component involved in cardholder data processing.
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 risk assessment.	CA PAM enables organizations to review logs and recordings (with DVR-like playback). Since all attempted policy violations are logged, CA PAM enables organizations to focus review efforts on the administrative sessions where attempted policy violations occurred and then spot-check other sessions for irregularities.

SECTION 3

Conclusion

As the PCI DSS version 3.2 regulations become mandatory starting in February 2018, it's critical for organizations to consider scalable solutions that help them address ongoing compliance. For these to happen, the following factors need to be considered:

- **Scalable and highly-available.** Given that systems and applications that are under the purview of PCI DSS contain sensitive cardholder data, not only should these applications be highly available but the solutions securing them should be as well. So, any privileged access management solution should be highly scalable—not just to provide for authentication and authorization of users and their access but for session management and recording as well.
- **Extensible.** As more systems and applications can come under PCI DSS, depending on the growth of the business or the phases of deployment, any privileged access management solution should be easily extensible to include new infrastructure and applications, rapidly and efficiently. Moreover, as the number of users, systems and applications increase rapidly, manual monitoring of user activity becomes hard. Any privileged access solution needs to provide analytics-based risk mitigation strategies. It's very likely that privileged access management needs to be integrated with other solutions to provide comprehensive support for the standard, and is an important consideration.
- **Cost of ownership.** As the required functionality of the privileged access management solution increases, the cost of ownership over a period (typically 3–5 years) should not be prohibitive. For example, a privileged access management solution may be easy to start with just password vaulting, but PCI DSS requires more than that, including functionality such as password policies, authorization and session management and recording. If these are provided separately, organizations may need to consider infrastructure, skill sets and licensing, as well as deploying costs needs across each phase. Additionally, maintenance and integration costs can vary across each phase, rendering a low entry price for the initial phase that's unviable in future phases.

To learn more about how CA privileged access management solutions can benefit your organization, visit **ca.com/pam**

Connect with CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-298517_0817