CYBERARK®

Securing Privileged Accounts:

Meeting the Payment Card Industry (PCI) Data Security Standard (DSS) 3.0 with CyberArk Solutions

Contents

Executive Summary

Obligations to Protect Cardholder Data

Any organization involved in payment card processing is well-aware of their obligations to protect cardholder data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). All entities that store, process or transmit cardholder data and/or sensitive authentication data, including merchants, processors, acquirers, issuers, and service providers are covered by PCI DSS. It provides a baseline of technical and operational requirements designed to protect cardholder data. The requirements apply to all system components included in or connected to the cardholder data environment.

The latest version of PCI DSS, Version 3.0, published in November 2013, is geared towards moving organizations from mere compliance to more comprehensive security approaches. This includes specific recommendations for making PCI DSS part of everyday business processes and monitoring the effectiveness of security controls on an on-going basis. The new version enables more flexibility in implementing the requirements and underscores the importance of shared responsibility when working with third-parties. All entities covered by PCI DSS must align with PCI DSS 3.0 by December 31, 2014.[1]

1 Some of the changes are future dated requirements that are best practices until July 1, 2015.

PCI and Privileged Accounts

Securing privileged accounts is one of the most important aspects of protecting cardholder data and complying with PCI DSS. Why?

PCI DSS contains extensive requirements for securing privileged access.

Privilege is pervasive. Privileged accounts consist not only of IT administrator or superuser accounts but also hard-coded, embedded credentials found in virtually every piece of hardware and software across an organization.

Privilege is powerful. By hijacking an administrative account or exploiting an embedded credential, attackers or malicious insiders can for example, gain entry to a network, take control over transactions, access an entire credit card database, modify system configurations, change security settings on a server or router, and delete audit logs.

Privilege is pursued. Because privileged accounts provide high levels of access, they are specifically targeted. In fact, most advanced attacks exploit privileged accounts. To carry out a cyber-attack, a critical step is getting privileged access to a network, server, operating system, application, device, and/or database.

Therefore, it is no surprise that PCI DSS contains extensive requirements related to securing privileged accounts and strictly controlling and monitoring their use. PCI DSS Version 3.0 puts even more emphasis on these powerful accounts. For a summary overview of all PCI DSS requirements related to securing privileged access, see page 7. A complete listing can be found on page 10.

The Challenges of Securing Privileged Access

Given the volume and complexity of privileged accounts that exist throughout the cardholder data environment, it can be very difficult to secure them. The challenges are many.

Lack of Visibility and Control

Firstly, entities are often not aware of all of the privileged accounts within their cardholder data environment. It can be hard to keep track of them all. Every server, operating system, desktop, laptop, router, virtual machine, and so on, has an administrative account associated with it. Every appliance, application, script, and device has an embedded credential. Without full knowledge or control of privileged accounts, many organizations leave them exposed to attack.

No Accountability

Administrative accounts, such as administrator on a Windows server, Root on a UNIX server, or Cisco Enable on a Cisco device are typically shared or generic administrative accounts. This makes it hard to trace individual use of the accounts and restrict use to necessary job functions. In some cases, administrative credentials must be used not only by internal personnel but also external third-party vendors, making it even more difficult to track all user access and ensure accountability.

Vulnerable Hard-coded Passwords

In the course of day-to-day business operations, numerous applications, scripts, and services access various resources in order to retrieve, process, transmit and store cardholder data. To perform their designated tasks, these applications are granted use of privileged accounts, allowing profuse access to cardholder data that is traversing a network or sitting in a database. These embedded accounts are difficult to secure since credentials are typically hard-coded and in clear text within business critical applications.

Problematic Password Refresh

Without automation, changing passwords for privileged accounts commonly leads to disruption of IT operations or business processes. Password changes require supplying updated passwords to all administrators or systems that rely on privileged credentials to perform ongoing tasks. This often results in interruption of services. Therefore, passwords for administrative and embedded accounts are typically changed infrequently, if at all. This greatly increases the risk of exposure and renders privileged accounts more susceptible to compromise.

Arduous Manual Methods

Tracking and monitoring privileged access involves reviewing audit logs across a multitude of disparate systems and devices, making it hard to ensure that all privileged access to sensitive data is authorized. Relying on manual methods to control, manage, update, and monitor privileged accounts is costly and prone to error.

The Risk To Business

Organizations that fail to adequately secure privileged accounts and protect cardholder data face the risk of non-compliance with the PCI DSS. Non-compliance can be costly. Consequences include fines, penalties, increased transaction fees, and/or terminated business relationships. But it goes beyond non-compliance.

Insecure privileged accounts represent a serious vulnerability. Sophisticated attacks against the retail sector are increasing. As an example, compromised privileged credentials have been used in attacks affecting millions of credit card records. As part of their modus operandi, perpetrators go after privileged accounts in order to conduct their attacks. Without proper security controls, organizations are leaving their "keys to the kingdom" susceptible to compromise, increasing the risk of a data breach. A breach of cardholder data could jeopardize customer trust, ruin a company's reputation, and potentially trigger a lawsuit; all of which could be extremely costly.

CyberArk's Comprehensive Approach

As the trusted expert in privileged account security, CyberArk provides a comprehensive approach to help organizations comply with PCI DSS and protect the cardholder data environment. With CyberArk solutions, entities can implement effective security controls to:

- Locate, manage and control all privileged accounts – including full lifecycle management
- Ensure only authorized users have access to privileged accountsLocate, manage and control all privileged accounts – including full lifecycle management
- Track, monitor and record all privileged access – to sensitive servers, databases or virtual machines by internal users, resources, and third-parties
- Uniquely identify all administrative users and restrict their use of privileged accounts to necessary job functions
- Ensure vendor-supplied default passwords are changed and automate password changes for all privileged accounts
- Eliminate hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with no impact on application performance or business processes
- Analyze, detect and alert on anomalous privileged user behavior – enabling quick response by incident response teams

Key Benefits

CyberArk's patented Digital Vault™ technology, military-grade encryption, robust reliability, and tamper-proof audit logs are designed to meet the highest security and compliance standards. By deploying CyberArk solutions, organizations can meet the extensive requirements of PCI DSS related to privileged account security and reduce the risks of damaging and costly data breaches. Key benefits include:

- Protect all system components included in or connected to the cardholder data environment
  - CyberArk provides enterprise-class security solutions designed to seamlessly integrate with an organization's IT infrastructure, including all system components included in or connected to the cardholder data environment – from e-commerce servers to point of sale (POS) devices.
- Reduce workload and PCI compliance costs
  - With manual methods, it takes considerable effort to secure privileged accounts and track and monitor their use throughout the cardholder data environment. By implementing CyberArk solutions, entities can reduce the workload involved in administering their IT infrastructure, and can also reduce the cost of compliance assessments. CyberArk's centralized management and reporting capabilities enable Qualified Security Assessors (QSAs) to easily verify the management and control of privileged accounts, potentially reducing the need for validation sampling, etc. Automation also enables organizations to decrease or reassign staff to more productive work.
- Increase situational awareness and visibility over privileged access to cardholder data
  - With real-time session monitoring of privileged access and behavioral analytics of privileged user activities, organizations can detect and stop advanced external and internal attacks.
- Achieve consistent enforcement of policy
  - Organizations can replace ineffective and inefficient manual processes with reliable, automated solutions for protecting privileged access to cardholder data; CyberArk solutions enable single pane of glass administration - one place to set, manage, and monitor privileged account security policy and controls.
- Protect systems containing cardholder data, whether on-premises or in the cloud
  - Organizations can seamlessly integrate CyberArk solutions with traditional datacenters and cloud environments including operating systems, servers, databases, virtual machines, applications, firewalls, security systems, network devices, routers, and more.
- Realize a low total cost of ownership
  - CyberArk solutions are designed to flexibly adapt to any business process, seamlessly integrate with system components throughout a cardholder data environment out-of-the-box, and provide consolidated management, policy controls and reporting capabilities – resulting in low deployment and administration costs.
- Leverage existing investments
  - CyberArk solutions work in conjunction with an organization's existing security infrastructure for protecting cardholder data - such as directory, identity management, provisioning, security information and event monitoring (SIEM), and authentication systems; and data analytics platforms.
- Solve a pressing problem quickly and expand the solution cost effectively to meet growing business requirements
  - The CyberArk Shared Technology Platform serves as the foundation for all of CyberArk's products, allowing organizations to deploy a single, scalable platform for securing privileged access across an organization's evolving cardholder data environment.
- Address compliance with regulations and contractual obligations for adequate security measures
  - CyberArk solutions can help organizations not only to comply with PCI DSS but also meet requirements to secure privileged accounts as part of complying with many local, regional and sector laws and regulations (e.g. HIPAA, SOX, NIST, NERC) and upholding agreements with customers and business partners that demand an effective information risk management program.

Overview of PCI DSS 3.0 Requirements Regarding Privileged Access

Throughout the PCI DSS, there are requirements related to securing privileged accounts, including requirements for protecting system configuration settings and passwords, developing and maintaining secure applications, restricting access to cardholder data, identifying and authenticating access, and tracking and monitoring access. The table on page 10 provides a detailed list of requirements and how CyberArk products address them.

PCI DSS Version 3.0 underscores the importance of securing privileged accounts by adding clarifications and/or evolving requirements concerning changing default vendor passwords, protecting systems from malware, reinforcing least privilege, managing vendor access, using unique authentication credentials, monitoring accounts with root or administrative privileges, and identifying suspicious activity. The table below summarizes the requirements related to securing privileged accounts, highlighting some of the changes in PCI DSS 3.0, and describes how CyberArk products support the requirements.

The CyberArk Privileged Account Security Solution supports the following PCI DSS requirements:

Build and Maintain a Secure Network and Systems

Requirement 1

Install and maintain a firewall configuration to protect cardholder data.

CyberArk solutions support the installation and maintenance of a firewall configuration by ensuring that only authorized privileged users can gain access to the configuration.

Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters.

CyberArk solutions help organizations control all the system passwords and other security parameters throughout the cardholder data environment. Organizations can implement automated credential management to ensure default passwords are changed, system passwords are consistently and effectively managed; and security parameters are configured only by authorized privileged users.

PCI DSS 3.0 clarifies that changing vendor default passwords applies to all default passwords. With CyberArk solutions, entities can implement automatic password management for over 100 operating systems, databases, firewalls, network devices, virtual machines, websites, and cloud-based applications. Extensible support for additional systems is provided with unique plug-in architecture for fast integration.

Maintain a Vulnerability Management Program

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs.

CyberArk provides a solution to isolate, control and monitor privileged user access and activities for critical systems within the cardholder data environment. Isolation between an administrator's desktop and target systems reduces the risk of malware spreading to critical systems.

PCI DSS 3.0 changed the title of the requirement to reflect the intent, which is to protect all systems against malware, and added consideration for additional anti-malware solutions to supplement anti-virus software. CyberArk solutions can help organizations protect their most critical systems from malware, beyond what antivirus software can do.

Requirement 6

Develop and maintain secure systems and applications.

CyberArk solutions help meet the requirements for removing application accounts and enforcing separation of the development and production environment, with access controls.

Implement Strong Access Control Measures

Requirement 7

Restrict access to cardholder data by business need to know.

CyberArk solutions help organizations limit privileged access to system components and cardholder data to only those individuals whose job requires such privileged access.

PCI DSS 3.0 refocuses the requirement to restrict privileged user IDs to least privileges necessary. With CyberArk solutions, organizations can implement and enforce fine-grained least privilege policies; privileged users can only access the particular privileged IDs and credentials to which they have been granted access and therefore only perform tasks that are assigned to that privileged ID. Organizations can also assign individual authorized users specific command-level privileges based on their roles.

Requirement 8

Identify and authenticate access to system components.

For privileged accounts, CyberArk solutions enable organizations to uniquely identify every privileged user and application; and automate and secure all of the processes associated with using privileged credentials and managing their lifecycle.

PCI DSS 3.0 enhances the requirement to manage IDs used for remote vendor access, including reinforcing that access should be disabled when not in use. CyberArk solutions uniquely identify any third-parties (e.g. vendors) provided with a privileged account. The organization can specify the time period for which the vendor is allowed access and disable access when not in use.

PCI DSS 3.0 also clarifies that strong cryptography must be used to render authentication credentials unreadable. With CyberArk solutions, all privileged passwords are protected with strong encryption at rest and in transit (when supported by the endpoint).

PCI DSS 3.0 adds a new requirement for service providers with remote access to customer premises to use a unique authentication credential for each customer. Service providers can use CyberArk solutions to securely manage the privileged credentials they need for remote access to customer premises and ensure a unique password for each customer is used.

Regularly Monitor and Test Networks

Requirement 10 **Track and monitor all access to network resources and cardholder data.**

CyberArk solutions enable organizations to effectively implement automated controls for tracking and monitoring all privileged access to network resources and cardholder data.

PCI DSS 3.0 enhances the requirement to track and monitor accounts with root or administrative privileges. For systems protected with CyberArk solutions, organizations can reconstruct events involving the use of privileged credentials including the use of and changes to identification and authentication mechanisms through privileged access such as the creation of new accounts and elevation of privileges. A detailed audit trail provides auditors with a complete, searchable record of privileged sessions.

PCI DSS 3.0 also clarifies that logs must be reviewed to identify anomalies or suspicious activity and emphasizes that automated log reviews facilitate the log review process. CyberArk solutions generate a rich set of real-time data on privileged credential access and accountability and integrate with Security Information and Event Management (SIEM) and event log systems. With CyberArk Privileged Threat Analytics, organizations can compare real-time privileged account user activity to historical behavior in order to detect anomalies as they occur.

Requirement 11 **Regularly test security systems and processes.**

CyberArk solutions support testing security systems and processes by ensuring that only authorized privileged users can gain access to tools such as vulnerability scanning systems.

Maintain an Information Security Policy

Requirement 12 **Maintain a policy that addresses information security for all personnel.**

With CyberArk solutions, organizations can consistently implement and maintain policies and procedures for privileged access.

Addressing PCI DSS 3.0 Requirements Regarding Privileged Access

Requirements Mapping

The following table details how CyberArk solutions help organizations to meet the requirements pertaining to privileged access within PCI DSS Version 3.0.

NOTE: The list of requirements is provided as general summary information only and limited to a subset of the requirements pertaining to privileged access; entities should refer to the PCI DSS Version 3.0 publication for comprehensive guidance on the complete set of requirements. Explanations regarding CyberArk solutions and how they can help organizations to meet the requirements related to privileged access are also provided as general summary information only. Entities must work with their Qualified Security Assessors (QSAs) to determine if their particular security controls meet these and all PCI DSS requirements.

PCI DSS Requirement	Overview of Requirements Related to Privileged Access and Associated CyberArk Solution Capabilities
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	As part of installing and maintaining a firewall configuration, organizations must ensure that only authorized privileged users can gain access to the firewall configuration.
1.1 Establish and implement firewall and router configuration standards	With CyberArk solutions, organizations can ensure that only authorized privileged users can make changes to firewall and router configuration settings. (For detailed information on how CyberArk solutions secure privileged access to all systems including security systems, see requirement 2.2.)
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	There are a number of reasons that make it difficult to effectively and efficiently change all vendor-supplied default passwords and adequately mitigate vulnerabilities. First, default passwords exist on almost every piece of software and hardware throughout an IT environment, therefore the sheer volume can make it difficult to locate all of these accounts and ensure that all of the passwords have been changed before they were installed. Second, even if IT administrators do change the passwords before installation, they often use the same password across multiple systems. Password re-use on sensitive systems fails to sufficiently mitigate the vulnerability because if attackers break one password, they get them all. Third, changing the passwords once, from the default to another password, still leaves the organization with the vulnerability of a static password. Another challenge in meeting this requirement is ensuring that only authorized users can gain access to configuration settings and make changes to security parameters. This is essential for all system components but particularly key for virtualized environments. It only takes a few seconds to provision a new virtual machine or move a virtual machine to another physical host; there could be serious violations of configuration standards if unauthorized users can gain access.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.	With CyberArk solutions, entities can identify all system accounts within the cardholder data environment and ensure that all vendor-supplied default passwords have been changed to unique passwords that meet password strength requirements defined by organizational policy. Entities can implement automatic password management and policy enforcement for the entire lifecycle of privileged accounts for all systems across the cardholder data environment, including out-of-the-box credential management for over 100 operating systems, databases, firewalls, network devices, virtual machines, websites, and cloud-based applications. Extensible support for additional systems is provided with universal plug-in architecture for fast integration.

2.2 Develop configuration standards for all system components	CyberArk solutions support the development of configuration standards by ensuring that only authorized privileged users can gain access and make changes to configuration settings for all system components throughout the cardholder data environment, including security systems, operating systems, databases, and enterprise applications. Organizations can effectively enforce access restrictions by controlling access to administrative passwords. Passwords are stored using CyberArk's patented, ICSA certified Vaulting Technology®, which employs multiple built-in layers of security to protect privileged credentials. When systems are protected with CyberArk solutions, administrators have no knowledge of the administrative passwords for an added layer of security. "Dual Control" can specify that access to highly sensitive passwords or policies requires confirmation by one or more authorized users, greatly limiting the ability to make unauthorized system changes. With CyberArk solutions, all privileged access to system configurations can be monitored. A tamper-proof audit record enables organizations to track which individual privileged users use administrative passwords to access system configuration changes. Organizations can also monitor and record all of the privileged sessions involving changes to configuration settings. As organizations increase their use of virtualization, CyberArk solutions can help to ensure only authorized privileged users make permitted changes to virtual machines, hypervisors and other system components in virtual environments. CyberArk solutions provide a central command and control point for managing and monitoring all privileged access and activity across the datacenter including virtualized environments.
2.3 Encrypt all non-console administrative access using strong cryptography and use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access	CyberArk solutions help to ensure that all non-console administrative access is encrypted using strong cryptography. With CyberArk solutions, all administrative passwords are protected with strong encryption both in transit and at rest. SSL encryption is used to transfer information between the main interface and the digital vault where passwords are stored. The vault uses FIPS 140-2 validated cryptography. For systems protected with CyberArk solutions, organizations can ensure that only authorized privileged users access approved applications that are securely configured to access systems with cardholder data including the use of strong cryptographic protocols.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	Anti-virus programs offer limited effectiveness against malware. Because privileged account credentials provide profuse access to systems containing cardholder data, it is critical that organizations can adequately protect systems from malware through privileged access. CyberArk provides a solution to isolate, control and monitor privileged user access and activities for critical UNIX and Windows-based systems, databases and virtual machines. The solution acts as a jump server and provides a single access control point, preventing malware from jumping to a target system. Isolation between an administrator's desktop and target systems eliminates the risk of malware spreading to critical systems. With CyberArk solutions, organizations can also record keystrokes and mouse clicks for continuous monitoring, enabling detection of malicious activity.
Requirement 6: Develop and maintain secure systems and applications	In meeting these requirements, one of the difficulties is dealing with passwords that are hard coded in applications, as these represent a major security vulnerability. They can be hijacked and exploited by attackers to gain privileged access. As part of conducting day-to-day business operations, many applications need access to resources in order to retrieve, process, transmit and store cardholder data. Another difficulty is effectively enforcing access controls for separating development/test environments from production environments. This requires the implementation of adequate access controls for privileged users.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers	CyberArk solutions provide automated application credential management, authenticating applications and allowing them to access resources by eliminating embedded application credentials. Instead of using hard-coded passwords, applications use credentials stored in the CyberArk Digital Vault without any impact to application performance or downtime. The solution provides centralized policy management and logging of all application access to resources.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls	With CyberArk solutions, organizations can ensure that only authorized users gain access to the development/test or production environments. Organizations can effectively enforce access restrictions by controlling access to administrative passwords. Passwords are stored using CyberArk's patented, ICSA certified Vaulting Technology®, which employs multiple built-in layers of security to protect privileged credentials. The patented digital vault technology inherently supports separation of duties. The vault is divided into safes that are accessed by users based on their specific permissions and without knowledge of the existence of other safes.

Requirement 7: Restrict access to cardholder data by business need to know	In restricting access to cardholder data to a business need to know, organizations must pay particularly close attention to the use of privileged accounts. Privileged users such as IT administrators are granted a high-level of access within the cardholder data environment. Without adequate restrictions on the use of privileged accounts, a malicious insider or attacker can use a privileged account to gain broad access to systems, applications, or databases containing cardholder data.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access	CyberArk solutions help organizations limit privileged access to system components and cardholder data to only those individuals whose job requires such privileged access. Access is restricted by controlling access to administrative passwords. Passwords are stored using CyberArk's patented, ICSA certified Vaulting Technology®, which employs multiple built-in layers of security to protect privileged credentials. All use of privileged credentials to access system components and cardholder data is tracked and monitored.
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	With CyberArk solutions, all privileged account information is held within the digital vault. Defining access needs for each role is facilitated by the use of safes within the vault; group managers are provided with restricted access to account information for their particular workgroup. For establishing conditions for group or role membership, organizations can leverage the group structure already created in their LDAP database such as Active Directory.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities	CyberArk enables organizations to restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities. With CyberArk solutions, organizations can implement and enforce fine-grained least privilege policies; privileged users can only access the particular privileged IDs to which they have been granted access and therefore only perform tasks that are assigned to that privileged ID. Organizations can also assign individual authorized users specific command-level privileges based on their roles. Workflows such as dual approval of password usage, email notifications and ticketing system integration for ticket validation and reasoning are just some of the many workflows that can be implemented to support least privilege.
7.1.3 Assign access based on individual personnel's job classification and function	CyberArk solutions provide granular account control for privileged identities; in addition to group and role membership, additional privileges and attributes can be specified for individual accounts.

7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed	CyberArk solutions help establish an access control system for privileged access to system components for multiple users. Organizations can automatically enforce privileged access rights such that only privileged users can gain access to privileged credentials and their credentials only allow them to access the information or system resources they are specifically entitled to.
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties	With CyberArk solutions, organizations can consistently implement policy and operational procedures for restricting privileged access to cardholder data.
Requirement 8: Identify and authenticate access to system components	To identify and authenticate access to system components, it is critical that organizations ensure unique identification (ID) of each individual person and application for privileged accounts which have powerful access rights. Organizations must be able to trace all privileged account activity to known and authorized users and processes. Shared administrative accounts such as Administrator on a Windows server, Root on a UNIX server, or Cisco Enable on a Cisco device represent a particularly thorny problem. With shared accounts, it is very difficult to ensure individual accountability for the use of the administrative credentials. Another key aspect of meeting this requirement is effectively managing and securing privileged accounts to ensure proper identification and authentication for all privileged access to system components. It can be difficult for organizations to ensure that these accounts are adequately managed and secured across the organization and throughout the entire lifecycle of each account.
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components	CyberArk automated solutions enable organizations to consistently implement policy and procedures to ensure proper identification management for privileged access by administrators on all system components.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data	Through the CyberArk Privileged Account Security Solution, all privileged users are assigned a unique ID, including each individual person and application.

8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects **8.1.3** Immediately revoke access for any terminated users **8.1.4** Remove/disable inactive user accounts at least every 90 days	CyberArk's comprehensive Privileged Account Security Solution seamlessly integrates with enterprise directories to automatically implement organizational policy. All account information is held within the CyberArk patented Digital Vault™. Through LDAP integration, any account changes – including addition, deletion, and modification of user IDs – is automatically propagated to the account information held in the vault. Upon termination, once-privileged users are removed from the directory, and all privileged access is immediately revoked. Any inactive privileged accounts removed or disabled from the directory are automatically removed/disabled from the vault.
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	CyberArk solutions uniquely identify any third-parties (e.g. vendors) provided with a privileged account and provide the ability to grant access without revealing any privileged passwords. The organization can specify the time period for which the vendor is allowed access to the vault and disable access when not in use. The system can be set up to issue a one-time password so that every time an account is used, a new password is issued. Organizations can also do real-time monitoring of privileged sessions. Further, non-organizational users who remotely connect to the digital vault connect through a proxy, so their session is encrypted and isolated from the internal network, mitigating third-party risks. The solution also integrates with Security Information and Event Management (SIEM) and event log systems for complete correlational analysis.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts	With CyberArk solutions, privileged users who fail authentication to the vault are locked out, preventing access to privileged credentials. Users are locked out until enabled by an administrator.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID **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	Organizations can require re-authentication for privileged users or applications based on time-frames or when users request to initiate additional sessions. As well, privileged sessions can be disconnected when a threshold (i.e. 15 minutes) is reached.

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

CyberArk solutions help organizations to ensure proper authentication for privileged access by administrators on all system components. Organizations can secure all of the processes associated with using privileged credentials and manage the credentials throughout their lifecycle.

To access privileged credentials in the digital vault, CyberArk solutions support a range of authentication methods, including: passwords, PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions.

All privileged passwords in the vault are protected with strong encryption both at rest and in transit (when supported by endpoint.)

The solution includes flexible and centralized password policy management for all privileged accounts across an organization including password aging, complexity, versioning and archiving. Organizations can set policy for privileged password format, including the requirements for a minimum length, and numeric and alphabetic characters; and can ensure passwords are unique. Password changes are automated based on an organizationally-defined time-frame, enabling organizations to schedule password changes including after every use, and enforce time limitations on passwords for all privileged users.

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components

8.2.3 Passwords/phrases must meet the following:

- Require minimum length of at least seven characters
- Contain both numeric and alphabetic characters

8.2.4 Change user passwords/passphrases at least every 90 days

---

8.3 Incorporate two-factor 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)

For remote access by privileged users (such as administrative or vendor support personnel), CyberArk solutions support a range of two-factor authentication methods to access the digital vault, including: PKI, tokens, OTP solutions, and smart cards. Furthermore, CyberArk solutions can be used to secure, control and monitor all remote access by privileged users. Organizations can fully control who can access systems remotely, ensure they use the proper two-factor authentication to gain entry, and monitor the sessions in real-time.

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

The CyberArk Privileged Account Security Solution helps organizations address the risks of group, shared, or generic IDs and passwords. When it is infeasible for an organization to disable or remove accounts such as Administrator on a Windows server, Root on a UNIX server, or Cisco Enable on a Cisco device, CyberArk solutions can be used to centrally secure, manage and track shared credentials across an organization, including ensuring individual accountability for the use of the administrative credentials.

Access to all administrative credentials is strictly controlled. Authorized administrators must use a unique user ID and password to login into the digital vault and gain access to the shared credential. CyberArk solutions link the unique identity of the administrator to their use of the shared credential. The solutions allow granular assignment of administrative privileges. All actions performed using the shared credential can be monitored and recorded. This includes continuous monitoring of all command-level activity in a privileged session, providing detailed visibility of privileged session activities and creating accountability for privileged users.

With CyberArk solutions, administrators have no knowledge of the shared passwords, greatly reducing the risk of exposure. The shared credential is stored using CyberArk's patented, ICSA certified Vaulting Technology®, which employs multiple built-in layers of security to protect privileged credentials.

8.5.1 Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer

Service providers can use the CyberArk Privileged Account Security Solution to securely manage the privileged credentials they need for remote access to their customers' premises. Complete privileged password management and protection is provided including automatically generating a unique password for each customer, periodically updating passwords according to policy (as frequently as after every use), restricting access to passwords to authorized users, and safeguarding passwords with strong encryption.

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)	With CyberArk solutions, organizations can restrict all privileged access to databases containing cardholder data to ensure that only authorized users or applications can gain access. To gain access to the database, privileged users such as database administrators must log in to the digital vault in order to access the privileged credentials to the database. For application access, CyberArk provides automated application credential management and access control which effectively eliminates embedded application credentials. To access a database, an application must first have authorized access to the privileged credentials in the vault. To gain access to the credentials, an application is authenticated using advanced authentication methods, based not only on ID and password but also on specific application characteristics including the server it resides on, the operating system it uses, and a crypto "fingerprint." Organizations can ensure only authorized applications with the appropriate ID and characteristics can access a database. Besides enhanced secure authentication, the solution provides periodic password refresh with no system downtime, centralized policy management, logging of all access to resources and a secure cache mechanism in the event of a network outage.
Requirement 10: Track and monitor all access to network resources and cardholder data	It can be difficult for organizations to effectively and efficiently track and monitor all privileged access to network resources and cardholder data.
10.1 Implement audit trails to link all access to system components to each individual user	With CyberArk solutions, privileged users and applications are uniquely identified and their activities logged, ensuring full accountability for individuals regarding privileged actions. Logs are securely stored in a tamper-proof vault.
10.1 Implement audit trails to link all access to system components to each individual user **10.2** Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual user access to cardholder data **10.2.2** All actions taken by any individual with root or administrative privileges **10.2.3** Access to all audit trails **10.2.4** Invalid logical access attempts	CyberArk solutions enable organizations to implement automated audit trails for privileged access to all system components. A universal connector allows organizations to monitor privileged access across the cardholder data environment, including for networks, servers, hypervisors, databases, applications, and more. The solutions provide continuous monitoring and recording of all privileged activity. Privileged session recordings include DVR style playback of sessions for event analysis, keystroke logging of SSH sessions, detailed session auditing for Windows, and SQL commands for Oracle sessions. For systems protected with CyberArk solutions, organizations can reconstruct events involving the use of privileged credentials. This can include all privileged access to cardholder data, all actions taken by any individual with root or administrative privileges, privileged access to all audit trails, invalid logical access attempts by privileged credentials, and the use of and changes to identification and authentication mechanisms through privileged access such as the creation of new accounts and elevation of privileges. A detailed audit trail provides auditors with a complete, searchable record of privileged sessions.

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 **10.2.6** Initialization, stopping, or pausing of the audit logs **10.2.7** Creation and deletion of system-level objects	With centralized management, the solution provides a single pane of glass for auditors to access information such as when privileged passwords are retrieved from the vault, changed, and used to execute privileged operations.
10.3 Record at least the following audit trail entries for all system components for each event: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6** Identity or name of affected data, system component, or resource	CyberArk solutions track all privileged actions by individual privileged users and applications. Content of event logs can be configured to include information on user identifiers, event descriptions, date and time, success/fail indicators, origination of event, identity or name of affected data, system component or resource, and more.
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: **10.4.1** Critical systems have the correct and consistent time **10.4.2** Time data is protected **10.4.3** Time settings are received from industry-accepted time sources	The CyberArk Digital Vault can be synchronized to the enterprise time source ensuring that the vault's timestamps (such as those on audit records) correspond to the system time.

10.5 Secure audit trails so they cannot be altered

10.5.1 Limit viewing of audit trails to those with a job-related need

10.5.2 Protect audit trail files from unauthorized modifications

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter

With CyberArk solutions, audit trails are protected with AES 256 cryptographic storage in a tamper-proof vault that is FIPS 140-2 certified. Access to the audit logs can be restricted to those with a job-related need. The audit records are centralized and audit events can be sent to another system for back up via the syslog protocol.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity

Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement

The CyberArk Privileged Account Security Solution generates a rich set of real-time data on privileged credential access and accountability, as well as complete, command-level data or live session views on exactly what is happening during a privileged session. Integrating with the world's leading solutions for event correlation and management, this information is readily available to security operations teams to help identify and triage suspicious privileged activity, and stop attacks. The solution integrates with Security Information and Event Management (SIEM) and event log systems including HP ArcSight, McAfee ESM, IBM/QRadar and RSA enVision for complete correlational analysis, including support for Syslog and XSL schema.

CyberArk also provides Privileged Threat Analytics, which uses proprietary algorithms to call attention to the most menacing of threats: those aimed at privileged accounts. CyberArk Privileged Threat Analytics compares real-time privileged account activity to historical behavior in order to detect anomalies as they occur. These anomalies are then correlated to immediately determine whether they reveal malicious intent. By applying patented analytic technology to a rich set of privileged account behavior, the CyberArk Privileged Threat Analytics solution produces highly accurate and immediately actionable intelligence, allowing incident response teams to respond directly to the attack. In addition to a proprietary dashboard built into the system, data and alerts from CyberArk Privileged Threat Analytics can be integrated into an organization's existing SIEM system. The analytics on fine-grained privileged user behavior improves the effectiveness of the SIEM system by enabling targeted alerts on privileged account risks.

10.6.1 Review the following at least daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions

---

10.6.2 Review logs of all other system components periodically, based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment

10.6.3 Follow up exceptions and anomalies identified during the review process

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)	CyberArk solutions can be configured to retain audits for any length of time and support any audit storage size.
10.8 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties	CyberArk solutions enable organizations to effectively implement policies and operational procedures for monitoring all privileged access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes	Organizations are required to frequently test systems, including running vulnerability scans. The scanning systems must be protected from unauthorized access.
11.2 Run internal and external network vulnerability scans at least quarterly	CyberArk solutions help ensure that only authorized privileged users can gain access to the vulnerability scanning systems.
Requirement 12: Maintain a policy that addresses information security for all personnel	Manual procedures can make it difficult to consistently and effectively maintain a security policy for privileged access.
12.1 Establish, publish, maintain, and disseminate a security policy	With CyberArk's automated solutions, organizations can consistently and effectively maintain a policy for privileged access to cardholder data. Pre-defined policies and workflows help streamline implementation of controls, built-in audit-ready reports enable efficient reviews, and flexible architecture provides support for updating controls. For privileged access, CyberArk solutions simplify the process of transforming business policy and procedures into technical settings; the policy can be easily managed and understood by an organization's stakeholders, including security operations, risk officers and auditors.

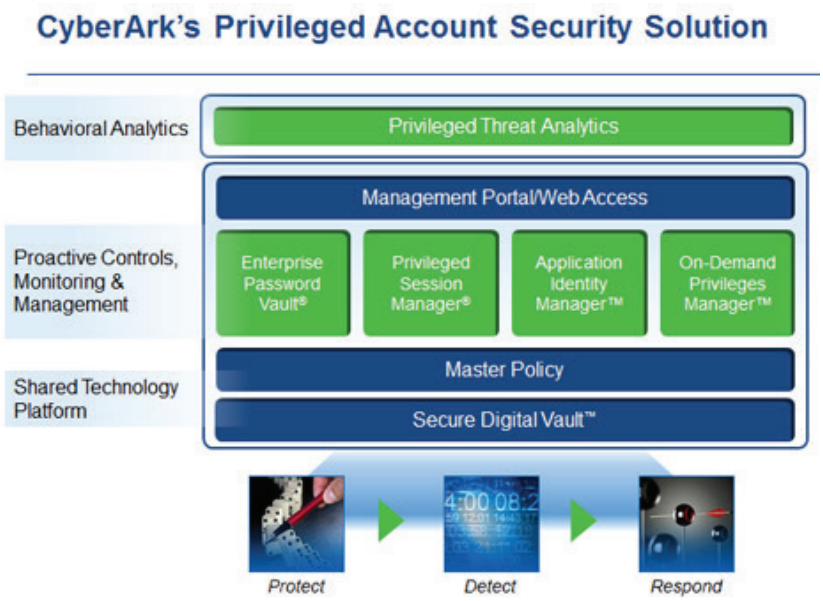
Conclusion

For all organizations involved in the payment processing industry, protecting privileged access is an essential part of meeting PCI requirements. Version 3.0 of the standard further enhances requirements related to privileged access. Because privileged accounts are extremely useful in conducting cyber-attacks, they are specifically targeted by cyber criminals and malicious insiders. Therefore in today's escalating threat landscape, securing privileged accounts is critical not only for meeting PCI requirements but also for reducing the risk of costly data breaches. But the task can be daunting, given the volume and complexity of securing privileged accounts for all system components included in or connected to the cardholder data environment. CyberArk's automated solutions can help entities to effectively and efficiently secure privileged access. The solutions are enterprise-proven in large and mid-sized organizations. CyberArk is the trusted expert in privileged account security.

Appendix: CyberArk Solutions

Privileged Account Security Solution

CyberArk is the trusted expert in privileged account security. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for on-premise, hybrid cloud and OT/SCADA environments.



Enterprise Password Vault® fully protects privileged credentials based on privileged account security policy and controls for who can access which credentials, and when.

Privileged Session Manager® isolates, controls, and monitors privileged user access as well as activities for critical UNIX, Linux, and Windows-based systems, databases, and virtual machines.

Privileged Threat Analytics™ analyzes and alerts on previously undetectable anomalous privileged user behavior enabling incident response teams to disrupt and quickly respond to an attack.

Application Identity Manager™ eliminates hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with no impact on application performance.

On-Demand Privileges Manager™ allows for control and continuous monitoring of the commands super-users run based on their role and task.

The CyberArk Privileged Account Security Solution is built on a common, shared technology platform that delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and the secure CyberArk Digital Vault™. The individual products in the CyberArk Privileged Account Security Solution integrate with the shared platform, enabling organizations to centralize and streamline management.

To help organizations get started with their privileged account security project, CyberArk offers a free assessment tool, CyberArk DNA™ (Discovery and Audit) that discovers and identifies privileged accounts throughout an enterprise. With a clear record of all service accounts, devices, and applications, CyberArk DNA helps organizations achieve an understanding of the size and magnitude of their privileged account security risk.