

Cyber-Ark® Software and the PCI Data Security Standard

ENTERPRISE PASSWORD VAULT® (EPV)



How Enterprise Password Vault Helps to Meet Key Requirements within the PCI DSS

The PCI DSS – Cyber-Ark’s View

The Payment Card Industry Data Security Standard (PCI DSS) defines security measures to protect cardholder information that must be implemented by processors, merchants and service providers.

The PCI DSS encompasses many aspects of network and data security. Its implementation implies development and adoption of security policies, the use of various security technologies and products as well as the adaptation of existing systems to use these technologies. As a result of the “lack of existence” of any single product to address all aspects of the PCI DSS, compliance can be a daunting task.

Cyber-Ark’s Enterprise Password Vault (EPV) creates a centralized point for enterprises to achieve exceptional security, streamline updates, enhance maintenance, and ensure compliance with government regulations across all types of privileged, shared and application passwords. These privileged identities can be found in routers, servers, databases, workstations and embedded in applications. EPV allows you to control the power within your organization by managing and securing all activities and logs associated with privileged passwords and shared accounts.

Enterprises should be looking for solutions that solve a broad spectrum of PCI DSS compliance issues while simultaneously eliminating any new security concerns. Furthermore, the PCI DSS requirements can be leveraged by enterprises to not only improve their security measures but also improve overall business processes and achieve return on investment (ROI) – which goes beyond compliance and security.

How Enterprise Password Vault Addresses the Specific Points of PCI DSS

Cyber-Ark products are built on top of their patented Vaulting® Technology -- equivalent to a physical safe, only in the digital world. The Cyber-Ark Vault allows organizations to secure data from end-to-end using multiple security layers, including Firewall, Data Access Control and End-to-End Encryption. To that end, Cyber-Ark’s

“

Cyber-Ark’s EPV addresses the business concerns and regulatory mandates for sensitive document security by providing a centralized secure repository and sharing platform for an organization’s most highly sensitive information ”



57 Wells Avenue
Suite 20A
Newton, MA 02469
P: 617.965.1544
E: sales@cyber-ark.com
W: www.cyber-ark.com

“

The focus on PCI DSS compliance is increasing each and every day, making it incumbent upon processors, merchants and service providers to do all they can to reach compliance as quickly and efficiently as possible. ”

Enterprise Password Vault (EPV) solution complies with many sections of the PCI DSS including: storage, in transit encryption, restricted access on a need-to-know basis, unique ids and comprehensive auditing. (See Appendix A for more details).

Cyber-Ark Enterprise Password Vault

- Enables organizations to secure, manage, automatically change and log activities associated with all types of Privileged Passwords (i.e. System Administrator on a Windows server, Root on a UNIX server, Cisco Enable on a Cisco device) as well as embedded passwords found in applications, scripts and application servers.
- Defines the storage, reset parameters and usage policies of passwords as well as personalizes administrative access that is usually carried with generic shared accounts, such as root or DBA users (meeting requirements 2.1, 10 and 10.1).
- Eliminates the usage of clear-text, hard-coded passwords within application code as required by section 6.3.6 of the PCI DSS.
- Streamlines IT processes and greatly improves the efficiency and security of IT to the organization (related to password management and password resets that otherwise may consume substantial resources).
- Provides the most secure location for passwords, documents and files containing such data and addresses most of the above-mentioned requirements (Section 3 of the PCI DSS)
- Helps achieve other systems' compliance, by, for example, securely storing encryption keys from other systems within the Vault as well.

Summary

The focus on PCI DSS compliance is increasing each and every day, making it incumbent upon processors, merchants and service providers to do all they can to reach compliance as quickly and efficiently as possible. The Enterprise Password Vault, and other Digital Vault-based solutions from Cyber-Ark Software answers to most of the specific PCI requirements around passwords and data security. By implementing these solutions, and the associated best practices approaches for privileged accounts and highly sensitive information, will greatly enhance many companies overall security posture and their compliance with PCI DSS.



57 Wells Avenue
Suite 20A
Newton, MA 02469
P: 617.965.1544
E: sales@cyber-ark.com
W: www.cyber-ark.com

Regulation requirement	How Cyber-Ark helps
<p>2 Do not use vendor-supplied defaults for system passwords and other security parameters.</p>	<p>Cyber-Ark Enterprise Password Vault provides a secure location for storing and sharing sensitive and powerful passwords across the enterprise.</p>
<p>2.1 Always change the vendor-supplied defaults before you install a system on the network.</p>	<p>The Enterprise Password Vault periodically resets and synchronizes passwords on servers, applications and appliances.</p>
<p>3 Protect stored data.</p>	<p>The most fundamental concept of Cyber-Ark Vault is its secure storage. The Vault provides comprehensive environment to securely store sensitive data. With its firewall, strong authentication, session encryption, storage encryption, extensive auditing, access control, dual control and other security measures, the Vault provides the ultimate environment to ensure the security and confidentiality of any type of file or document.</p>
<p>3.1 Keep cardholder information storage to a minimum. Limit your storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.</p>	<p>Information stored within the Enterprise Password Vault is subjected to retention period rules and will be deleted upon the expiration of this period.</p>
<p>3.4 Render sensitive cardholder data unreadable anywhere it is stored, by using (among others) strong cryptography, such as Triple-DES 128-bit or AES 256-bit with associated key management processes and procedures.</p>	<p>Data stored within the Enterprise Password Vault is encrypted and signed using AES 256-bit and SHA-1.</p> <p>The Vault seamlessly protects and manages encryption keys.</p>
<p>3.5 Protect encryption keys against both disclosure and misuse:</p> <p>3.5.1 Restrict access to keys to the fewest number of custodians necessary.</p> <p>3.5.2 Store keys securely in the fewest possible locations and forms.</p>	<p>Cyber-Ark Enterprise Password Vault internally manages its encryption keys. Each data item is encrypted with a unique encryption key.</p> <p>Only the relevant encryption keys are provided to authenticated and authorized users (req. 3.5, 3.5.1, 3.5.2).</p>

Regulation requirement	How Cyber-Ark helps
<p>3.6 Fully document and implement all key management processes and procedures, including:</p> <p>3.6.1 Generation of strong keys</p> <p>3.6.2 Secure key distribution</p> <p>3.6.3 Secure key storage</p> <p>3.6.4 Periodic key changes</p> <p>3.6.5 Destruction of old keys</p> <p>3.6.6 Split knowledge and dual control of keys (so that it requires 2 or 3 people, each knowing only their part of the key, to reconstruct the whole key).</p> <p>3.6.7 Prevention of unauthorized substitution of keys</p>	<p>Cyber-Ark Enterprise Password Vault fully manages encryption keys for stored data (req. 3.6), including:</p> <p>Generation of strong keys (req. 3.6.1)</p> <p>Keys are securely distributed over an encrypted channel to authenticated and authorized users (req. 3.6.2).</p> <p>Keys are securely stored within the Vault, benefiting from all of the Vault's security layers (req. 3.6.3).</p> <p>Encryption keys can be changed periodically (req. 3.6.4).</p> <p>Encryption keys are used only once – every data item has a unique key (req. 3.6.5).</p> <p>The Dual Control feature ensures selected data is subject to additional confirmation before leaving the Vault (req. 3.6.6).</p> <p>Encryption keys are stored within the Vault and can't be substituted manually (req. 3.6.7).</p>
<p>4 Encrypt transmission of cardholder and sensitive information across public networks.</p> <p>Use encryption techniques (at least 128 bit) such as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC), etc. to safeguard sensitive cardholder data during transmission over public networks.</p>	<p>All data transmitted to and from the Enterprise Password Vault is encrypted and digitally signed using AES-256 and SHA-1.</p>
<p>6 Develop and maintain secure systems and applications.</p> <p>6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.</p>	<p>The Enterprise Password Vault is used to remove clear-text, hard-coded passwords from application code.</p>

Regulation requirement	How Cyber-Ark helps
7 Restrict access to data by business need-to-know.	Information stored in Cyber-Ark Enterprise Password Vault in a highly departmentalized manner. Only authenticated users can access data and only based on their authorizations (req. 7, 7.1).
7.1 Information stored in Cyber-Ark Enterprise Password Vault in a highly departmentalized manner. Only authenticated users can access data and only based on their authorizations.	
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Each user of the Vault is assigned with an individual account and can access only data he or she is permitted to (req. 7.2).
8 Assign a unique ID to each person with computer access	Each user of the Enterprise Password Vault is assigned with an individual account (req. 8, 8.1).
8.1 Identify all users with a unique username before allowing them to access system components or cardholder data.	
8.2 Employ at least one of the methods below, in addition to unique identification, to authenticate all users: Password, Token devices (e.g., SecureID, certificates, or public key), Biometrics.	Cyber-Ark Vault supports strong authentication mechanisms that can be based on passwords or tokens (req. 8.2, 8.5)
8.3 Implement 2-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.	The Vault also supports 2-factor authentication (req. 8.3).
8.4 Encrypt all passwords during transmission and storage, on all system components.	The authentication process to the Vault is secure and the credentials (e.g. password) are encrypted (req. 8.4)
8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components.	Additionally, Cyber-Ark's Enterprise Password Vault can be used to protect and periodically change various passwords across the organization (req. 8.4, 8.5).

Regulation requirement	How Cyber-Ark helps
<p>10 Track and monitor all access to network resources and card-holder data.</p>	<p>Access to data within the Enterprise Password Vault is logged (req. 10).</p>
<p>10.1 Establish a process for linking all access to system components (especially those done with administrative privileges such as root) to an individual user.</p>	<p>Enterprise Password Vault enforces personalization of shared administrative accounts (such as root and DBA accounts) and guarantees logging is on an individual level (req. 10.1).</p> <p>Each user of the Vault is assigned with an individual account, thus audit logs are always personal (req. 10.1).</p>
<p>10.2 Implement automated audit trails to reconstruct the following events, for all system components:</p> <p>10.2.1 All individual user accesses to cardholder data.</p> <p>10.2.2 All actions taken by any individual with root or administrative privileges.</p> <p>10.2.3 Access to all audit trails.</p> <p>10.2.4 Invalid logical access attempts.</p> <p>10.2.5 Use of identification and authentication mechanisms.</p> <p>10.2.6 Initialization of the audit logs.</p> <p>10.2.7 Creation and deletion of system level objects.</p> <p>10.3 Record at least the following audit trail entries for each event, for all system components: User identification; Type of event; Date and time; Success or failure indication; Origination of event; Identity or name of affected data; system component or resource.</p>	<p>Cyber-Ark Enterprise Password Vault logs every successful and unsuccessful events, including login, data access and administrative activities (req. 10.2, 10.2.1, 10.2.4, 10.2.5, 10.2.7).</p> <p>Audit trails are stored within the Vault and protected by it. Audit trails are encrypted and signed and can't be altered manually. Audit trail is maintained for a predefined period of time and can't be deleted before the retention period expires. Audit logs are backed up as part of the standard system backup procedures. Access to the logs is governed by access control (req. 10.2.3, 10.2.6, 10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.5, 10.7)</p> <p>Audit logs contain detailed information about the nature of the event, including acting user, type, data and time, success or failure and event origination (req. 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6)</p>

Regulation requirement

How Cyber-Ark helps

10.5 Secure audit trails so they cannot be altered, including the following: Limit viewing of audit trails to those with a job-related need; Protect audit trail files from unauthorized modifications; Promptly back-up audit trail files to a centralized log server or media that is difficult to alter; Use file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed without generating alerts.

10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.

About Cyber-Ark

Cyber-Ark™ Software is the leading provider of Privileged Identity Management (PIM) solutions or securing privileged user accounts and highly-sensitive information across the enterprise. Long recognized as an industry innovator for its patented Vaulting Technology™, Cyber-Ark's digital vault products include: The Enterprise Password Vault™ for the secure management of administrative, application and privileged user passwords; the Inter-Business Vault™, a secure infrastructure for cross-enterprise data exchange of highly-sensitive information, and the Sensitive Document Vault™ for secure storage and management of highly-sensitive documents. Cyber-Ark's Vaulting platform has been tested by ICSA Labs, an independent division of Cybertrust and the security industry's central authority for research, intelligence, and certification testing of security products. Cyber-Ark's award-winning technology is deployed by more than 300 global customers, including 100 of the world's largest banks and financial institutions. Headquartered in Newton, MA, Cyber-Ark has offices and authorized partners in North America, Europe and Asia Pacific. For more information, visit www.cyber-ark.com