

Cyber-Ark® Software and the PCI Data Security Standard

INTER-BUSINESS VAULT® (IBV)



“**Inter-Business Vault creates a multiple-layered information security infrastructure that is easy to use, simple to adopt and efficient to administer...**”

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 that 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 Inter-Business Vault (IBV) addresses the business concerns and regulatory mandates for the exchange and sharing of sensitive information between an enterprise and its business community. Based on our patented and ICISA validated secure Digital Vault technology, the Inter-Business Vault creates a multiple-layered information security infrastructure that is easy to use, simple to adopt and efficient to administer, all while providing the security, flexibility and detailed tracking capabilities missing from today’s plethora of one-dimensional encryption only based solutions.

How Inter-Business 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 Inter-Business Vault 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 Inter-Business Vault:

- Enables organization to secure and manage file transfers containing cardholder information to and from partners, customers and business units.
- Secures cardholder data in flat files (e.g. Excel files and other human-readable document files, machine-readable, transaction files) at rest and while in transit (requirements 3.4 and 4.1).
- Ensures only designated recipients have access to cardholder



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. ”

- information (requirements 3.5, 7.1 and 7.2).
- Provides separation of duties and blocks system and network administrators from accessing sensitive data (requirements 3.5, 7.1 and 7.2).
- Maintains secure, tamper-proof auditing and logging of all activities done with files containing cardholder data, including who “has” or “had” access to these files (requirements 10.2, 10.3, 10.5 and 10.7).
- Provides transparent encryption key management, mitigates any overhead in issuing, securing, distributing, revoking and destroying encryption keys (Requirement 3.6).
- Centralizes control of and streamlines file transfer processes while improving efficiency, providing operational simplicity and reducing risk.

Summary

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.

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 Inter-Business Vault and other Digital Vault-based solutions from Cyber-Ark Software answers to most of the specific PCI requirements around data security. By implementing these solutions, and the associated best practices approaches for highly sensitive information and privileged accounts, 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>1 Install and maintain a firewall configuration to protect cardholder data</p>	<p>Cyber-Ark Vault contains a built-in firewall with a predefined strict policy that protects the Vault and any data stored within. This feature eliminates the need to develop complex firewall policies for exchanging data with partners.</p>
<p>2 Do not use vendor-supplied defaults for system passwords and other security parameters</p> <p>2.1 Always change vendor-supplied defaults before installing a system on the network</p> <p>2.3 Encrypt all non-console administrative access</p>	<p>Cyber-Ark Vault does not have predefined, default passwords (req. 2.1).</p> <p>All communication, including non-console administrative access is encrypted and signed (req. 2.2).</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, object 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 Inter Business 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 Inter-Business Vault is encrypted and signed using AES 256-bit and SHA-1. 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 Inter Business Vault internally manages its encryption keys. Each data item is encrypted with a unique key. 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 Inter Business 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). Encryption keys are stored within the Vault and can't be substituted</p>
<p>4 Encrypt transmission of cardholder and sensitive information across public networks. 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 Inter-Business Vault is encrypted and digitally signed using AES-256 and SHA-1.</p>
<p>5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>Cyber-Ark Vault integrates with leading antivirus products to ensure that data transmitted in and out of the organization is virus free.</p>
<p>7 Restrict access to data by business need-to-know.</p> <p>7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.</p> <p>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</p>	<p>Information stores with Cyber-Ark's Inter Business Vault in a highly departmentalized manner. Only authenticated users can access data and only based on their authorizations (req. 7, 7.1).</p> <p>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).</p>

Regulation requirement	How Cyber-Ark helps
<p>8 Assign a unique ID to each person with computer access.</p> <p>8.1 Identify all users with a unique username before allowing them to access system components or cardholder data.</p> <p>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.</p> <p>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.</p> <p>8.4 Encrypt all passwords during transmission and storage, on all system components.</p> <p>8.5 Ensure proper user authentication and password management for non-consumer users and administrators, on all system components.</p>	<p>Each Inter Business Vault user is assigned an individual account (req. 8, 8.1).</p> <p>Cyber-Ark Vault supports strong authentication mechanisms that can be based on passwords or tokens (req. 8.2, 8.5).</p> <p>The Vault also supports 2-factor authentication (req. 8.3).</p> <p>The authentication process to the Vault is secure and the credentials (e.g. password) are encrypted (req. 8.4).</p>
<p>10 Track and monitor all access to network resources and cardholder data.</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>Access to all data within the Inter Business Vault is logged (req. 10).</p> <p>Cyber-Ark Inter Business Vault logs every successful and unsuccessful event, including login, data access and administrative activities (req. 10.2, 10.2.1, 10.2.4, 10.2.5, 10.2.7).</p>

Regulation requirement	How Cyber-Ark helps
<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>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 are 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>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.</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>
<p>10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.</p>	

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