

RSA enVision™ Platform

Payment Card Industry (PCI) Compliance

At a Glance

- Meets log monitoring and reporting mandates under Requirement 10 in PCI's 12-step process
- Captures All the Data™ from network, security, host, application and storage layers across the enterprise
- Analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization
- Provides the ability to automatically generate alerts based on non-compliance with specific regulations and the detection of unusual levels of activity

Sponsored by a collaboration between MasterCard, Visa, American Express, Diners Club and the Discover Card, the Payment Card Industry Standard (PCI) is an effort to protect consumer information and fight Internet fraud through required best practices for securing credit card data that is stored, processed or transmitted by an online retailer. All merchants who process or store credit card transaction data must comply with PCI regulations.



The Security Division of EMC

Objectives to Meet PCI Compliance

To achieve compliance, merchants and service providers must adhere to PCI security standards, which offer a single approach to safeguarding sensitive data for all card brands. The PCI security standard is a framework of twelve basic requirements supported by more detailed sub-requirements. Log monitoring and reporting is mandated under Requirement 10 in PCI's 12-step process that instructs companies on how to achieve compliance.

Specifically, PCI requires organizations to:

- Regularly monitor and test networks
- Track and monitor all access to network resources and cardholder data

The RSA enVision™ Platform automates this compliance requirement by creating mapped reports that allow organizations to capture and report on the logs from network, security, infrastructure and application-layer events. The Platform's reports provide your organization with a complete picture of network usage and audit trails for user identification, success and failure indication, origination of event and validation of user views of information.

To achieve those objectives, PCI requires that companies monitor and audit the following types of activities:

- Access Control monitors attempts to access anything on a company's systems including files, directories, database records or applications.
- Configuration Control monitors the configuration, policies and software installed on systems covered by a particular compliance regulation and all systems with access to that system.

- Malicious Software capabilities detect, collect and report malicious activities caused by viruses or other malicious code.
- Policy Enforcement verifies that all users are complying with regulations to reduce the change of accidental exposure of sensitive information.
- User Monitoring and Management creates a complete audit of the activities of non-employees with access to private data and takes steps to minimize the risk from compromised accounts.
- Environmental and Transmission Security involves the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measures such as VA scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured and done with the proper encryption levels.

(See chart for specific compliance reports generated for each regulation. While there are specific activities that are required to be monitored by PCI, auditors may investigate other areas such as Malicious Software, User Monitoring and Management and Environmental and Transmission Security categories if they see unusual or suspicious activities. For that reason, maintaining data in a readily assessable format is recommended. RSA enVision solution provides those capabilities.)

To achieve and maintain compliance in those areas, companies must use the following functions with respect to the data collected by the RSA enVision Log Management solution:

- Collect, Protect and Store data in a non-filtered, non-normalized fashion that is stored in an efficient and protected manner.
- Establish Baseline levels of activity for the entire system and network environment to define “normal activity” and detect unusual levels of activity.
- Report summary and detailed reports for the mandated periods of time.
- Alert companies to deviations from baseline activities and complex patterns of activity across multiple, disparate devices.

- Debug systems to correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
- Establish Incident Management capabilities for close monitoring and correction of violations to make sure they are recorded, escalated and corrected in a timely and thorough manner.

These functions ensure that the administrative, physical and technical control demanded by PCI regulations are maintained. RSA enVision solutions address all of the technical standards required.

The RSA enVision Internet Protocol Database

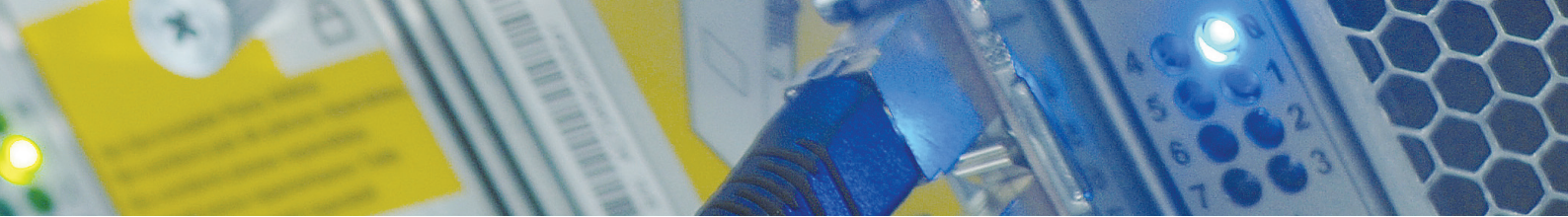
Using its advanced LogSmart Internet Protocol Database (IPDB) architecture that is deployed in hundreds of enterprises worldwide, the Platform is able to capture All the Data™ from network, security, host, application and storage layers across the enterprise. The LogSmart IPDB analyzes both real-time and historical data and presents information in views and reports designed to meet the far-ranging needs of everyone in your organization — from the IT department, to the security department, to the compliance and risk officers and executive management.

The benefits of the LogSmart IPDB include:

- Designed to store and work efficiently with unstructured data natively without any filtering or data normalization
- Maintains a digital chain of custody for all data which assures that once data is committed to the database, it can never be altered — unlike most data schemas used in RDBMS-based solutions
- No agents are required
- Distributed peer-to-peer architecture enables high scalability and performance

Compliance Alerts

The RSA enVision Platform provides the ability to automatically generate alerts based on non-compliance with specific regulations and the detection of unusual levels of activity. Such incidents trigger alerts so action can be taken to maintain compliance.



OBJECTIVE	PCI SECTION	REPORT TITLE	DESCRIPTION
Access Control	10.2.1	PCI – Individual User Accesses to Cardholder Data - Windows	This report displays all successful file access attempts to file objects in the the “Cardholder Data” device group.
Access Control	10.2.4	PCI – Invalid Logical Access Attempts - ACL Denied Summary	This report displays all access attempts that have been denied due to access control list restrictions.
Access Control	10.2.3	PCI – Access to All Audit Trails	This report displays all successful logins to enVision™.
Configuration Control	1.1.1, 1.1.8	PCI – Firewall Configuration Changes	This report displays all configuration changes made to firewalls within the PCI device group.
Configuration Control	1.1.9	PCI – Router Configuration Changes	This report displays all configuration changes made to routers within the PCI device group.
Configuration Control	2.1.1	PCI – Wireless Environment Configuration Changes	This report details all configuration changes made to wireless routers. PCI requires that all vendor defaults, including WEP keys, default SSID, password, SNMP community strings and disabling of SSID broadcasts, be changed before a wireless router be introduced to the payment-card environment.
Malicious Code Detection	5.2	PCI – Anti-virus Update Procedures	This report lists all update procedures for anti-virus systems.
Policy Enforcement	1.1.6	PCI – Traffic to Non-standard Ports – Detail	This report details all firewall traffic by port to the IP address specified as a run-time parameter where the port used is not directly justified by PCI.
Policy Enforcement	1.3.1, 1.3.2	PCI – Inbound internet traffic on non-standard ports - Detail	These reports list all inbound Internet traffic on non-standard ports within the PCI device group in detail and summary format
Policy Enforcement	1.3.6	PCI – Outbound Traffic Summary	This report summarizes all outbound traffic by destination. PCI requires that all outbound traffic be restricted to what is necessary for the payment-card environment.
Policy Enforcement	1.3.6	PCI – Outbound Traffic Detail by Source Address	This report details all outbound traffic for a specific internal IP address. The IP address in question should be entered as a run-time parameter.
Policy Enforcement	1.1.6	PCI – Traffic to Non-standard Ports – Summary	This report summarizes all firewall traffic by port by destination computer, where the port used is not directly justified by PCI.
Policy Enforcement	10.2.6	PCI – Initialization of Audit Logs	This report shows the initialization of audit logs in Windows, UNIX, Linux, AIX and HP-UX operating systems.
Policy Enforcement	10.2.7	PCI – Deletion of System-level Objects – Windows	This report shows the deletion of all system-level objects in monitored Windows systems. This report should be run against the “PCI” device group.
Policy Enforcement	1.1.5	PCI – Traffic by Port – PCI Device Group	This report summarizes all firewall traffic by port into the PCI device group.
User Monitoring	10.1	PCI – Administrative Privilege Escalation - Unix/Linux	This report displays all successful administrative privilege escalations on monitored Unix and Linux systems.
User Monitoring	10.2.2	PCI – All Actions by Individuals with Root or Administrative Privileges – Unix/Linux	This report displays all actions taken by users logged in as “root.” This report should be modified to include any additional usernames that have been granted full user monitoring administrative privileges in your environment.



OBJECTIVE	PCI SECTION	REPORT TITLE	DESCRIPTION
User Monitoring	10.2.2	PCI — All Actions by Individuals with Root or Administrative Privileges — Windows	This report displays all actions taken by users logged in as “Administrator.” This report should be modified to include any additional usernames that have been granted full administrative privileges in your environment.
User Monitoring	10.2.5	PCI — Use of Identification and Authentication Systems — RSA	This report lists all users accessing the PCI device group that authenticate using RSA authentication servers.
Environmental and Transmission Control	3.6.1, 3.6.4	PCI — Encryption Key Generation and Changes	This report details all the generation and period changing of encryption keys used in the secure storage and transfer of payment-card data.
Environmental and Transmission Control	4.1	PCI — Encrypted Transmission Failures	This report lists all cryptographic operations where the use of the cryptography failed or was disabled by the user.
Environmental and Transmission Control	6.1	PCI — Vendor-supplied Patch Application — Windows	This report lists all patch and service pack application to Windows systems.
Environmental and Transmission Control	6.1	PCI — Vendor-supplied Patch Application	This report lists all patch and service pack application to Windows systems.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

©2007 RSA Security Inc. All Rights Reserved.

RSA, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. Microsoft, Windows, Windows Mobile, and Internet Explorer are registered trademarks or trademarks of Microsoft Corporation. Palm is a registered trademark or trademark of Palm, Inc. Mozilla and Firefox are registered trademarks or trademarks of the Mozilla Foundation. Blackberry is a registered trademark or trademark of Research In Motion Limited in the U.S. and/or other countries. All other trademarks mentioned herein are the properties of their respective owners.



RSA Security Inc.
 RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

ENPCI DS 0407