

PCI and PA DSS Compliance Assurance with LogRhythm

Introduction

LogRhythm provides support for PCI compliance out-of-the-box as part of the PCI Compliance Package. The enterprise assets are categorized according to Network Security, Cardholder Data, Vulnerability Management, Access Control, Network Monitoring and Testing, and Information Security Policy. The collection, management, and analysis of log data are integral to meeting PCI audit requirements. IT environments consist of heterogeneous devices, systems, and applications, all reporting log data. The Payment Application Data Security Standard (PA DSS) is derived from PCI DSS, and its individual requirements align with PCI DSS requirements.

To ensure compliance with PCI requirements, information systems are monitored in real time. Investigations, Reports, and Alarm Rules are provided, allowing for immediate notification and analysis of conditions that are impacting the integrity of the organization's cardholder data. Areas of non-compliance can be identified in real-time. Additional Investigations, Reports, and Alarm Rules are provided as part of LogRhythm's standard Knowledge Base to further augment the usefulness of the log data. Reports can be generated as needed by the PCI Security Assessor and scheduled to run at pre-determined intervals. LogRhythm's PCI DSS Compliance Package can be used to help meet PA DSS standards as well. LogRhythm's extensive support for both commercial and custom payment applications enable comprehensive and efficient collection, processing, review and reporting of all log sources specified in both the PCI and PA data security standards.

Requirements

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS standards apply to all organizations that store, process, or transmit cardholder data and all affected organizations must be PCI compliant.

The PCI DSS standards are enforced by the founding members of the PCI Security Standards Council consisting of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The first PCI DSS standard was released on December 15, 2004 and its latest revision was released on October 1, 2008. LogRhythm is a participating organization in the PCI Security Standards Council and as such, will work with the Council to evolve the PCI Data Security Standard (DSS) and other payment card data protection standards.

Solution Summary

LogRhythm's PCI DSS Compliance Package provides specific Investigations, Alarms and Reports designed to meet PCI DSS reporting requirements. They are automatically associated with the correct PCI DSS asset categories ensuring only relevant information is included. Reports can be scheduled for periodic generation and delivery or generated on demand by the security officer and other LogRhythm users. Investigations and Alarms can be leveraged for immediate analysis of activities that impact the organization's cardholder data systems so areas of non-compliance can be identified in real-time.

LogRhythm Provides Automated Compliance Support for PCI and PA DSS

- **Build and Maintain a Secure Network**
Monitors firewalls and network protection systems such as IDS/IPS and UTM, as well as PCI mandated behavior such as removing default passwords.
- **Protect Cardholder Data**
Monitors user behaviour and configuration changes that may jeopardize the security of cardholder data.
- **Maintain a Vulnerability Management Program**
Monitors anti-malware and vulnerability management products for rapid exposure assessment, incident handling and response.
- **Strong Access Controls**
Monitors access to card holder systems and data and identifies and alarms on suspicious behaviour.
- **Monitor and Test Networks Regularly**
Establishes an automated audit trail for all system components as mandated by PCI DSS Requirements 10.2-10.7 and meets both the conditions and the spirit of these requirements.
- **Maintain an Information Security Policy**
Supports security best-practices, enabling organizations to meet PCI standards.



PCI DSS Dashboard

The table shows how LogRhythm’s PCI DSS Compliance Package addresses multiple sections of the standard and the additional benefits gained.

PCI DSS Requirement		Solution	LogRhythm Offering
PCI DSS 1: 1.1, 1.2, 1.3	Install and Maintain a Firewall Configuration to Protect Data	Collects logs from firewall devices to ensure and validate compliance.	Monitors all used services, protocols and ports, validates inbound and outbound traffic, and captures and alarms on event data related to network and firewall specific activity.
PCI DSS 2: 2.3	No use of Vendor-Supplied Security Parameter Defaults	Monitors the network for indications of improper behaviour and signs of weak security configurations.	Provides a record of all services used and can alarm on the use of non-encrypted protocols.
PCI DSS 3: 3.6.7	Protect Stored Cardholder Data	Provides monitoring of changes in the cardholder environment and can alarm on changes to security critical resources.	Alarms on actions that affect specific files or objects, such as the details of who, when and where if a cryptographic key is altered.
PCI DSS 4: 4.1, 4.1.1	Encrypt Cardholder Data Transmission Across Open Public Networks	Monitors network use to ensure that only the proper protocols are being used in the cardholder data environment.	Monitors and alerts on unauthorized or unencrypted services being used, and can report on detected wireless networks to help control access points.
PCI DSS 5: 5.2	Use and Update Anti-virus Software or Programs	Collects log data from antivirus solutions and can alarm on detected malware and compromises in the cardholder data environment.	Identifies operational errors from antivirus and antimalware applications, can detect when new signatures are installed, and alert on malware detected within the cardholder data environment.
PCI DSS 6: 6.1, 6.3, 6.5, 6.6	Develop and Maintain Secure Systems and Applications	Helps organizations develop and maintain secure systems and applications by correlating all log and event data, providing a centralized, comprehensive view of an organization’s security posture.	Monitors and reports on when and if critical patches are installed, and can report on the security posture, of commercial, custom and web applications in conjunction with other security devices.
PCI DSS 7: 7.1	Restrict Cardholder Data Access to Need-to-Know	Monitors access privilege assignments and suspicious data accesses.	Collects relevant data from access control systems, monitoring and validating access to cardholder data through account creation, object access, and privilege assignment and revocation.
PCI DSS 8: 8.1	Assign Unique IDs to Everyone with Computer Access	Identifies shared account usage in the network, including unobvious accounts with more than one user.	Reports on all user-account activity from account creation and activity to account removal. Alarming on default and shared account usage can provide real-time validation.
PCI DSS 10: 10.2, 10.3, 10.4, 10.5, 10.6, 10.7	Track and Monitor Access to All Network Resources and Cardholder Data	Automates collection, centralization and monitoring of logs from servers, applications, security and other devices, significantly reducing the cost of compliance.	Collects all access-related logs, maintaining a digital chain-of-custody to protect audit trails against unauthorized modifications. LogRhythm also provides discretionary access for optimal compliance controls.
PCI DSS 11: 11.4, 11.5	Regularly Test Security Systems and Processes	Collects logs from IDS/IPS devices to help ensure and validate compliance. File Integrity Monitoring capabilities can be used to directly meet requirement 11.5.	Risk-based prioritization and alerting reduces the cost of running IDS/IPS and monitors intrusion-related activity in real-time. File Integrity Monitoring tracks reads and modifies for critical files and directories.
PCI DSS 12: 12.9	Maintain an Information Security Policy Employees and Contractors	Provides centralized intelligence to support organizational security policies, including incident handling and response.	Easily expands beyond the cardholder data environment to provide support to other areas of the organization.

LogRhythm Headquarters

3195 Sterling Circle
Boulder, CO 80301
303-413-8745

LogRhythm EMEA

Siena Court, The Broadway
Maidenhead Berkshire SL6 1NJ
United Kingdom
+44 (0) 1628 509 070

LogRhythm Asia Pacific Ltd.

8/F Exchange Square II
8 Connaught Place, Central
Hong Kong
+852 2297 2812