LogRhythm

Solution Brief

PCI DSS Compliance

Eliminate Unnecessary Steps to Meet Compliance

Meeting all the payment card industry (PCI) compliance requirements is difficult for any organization. Each control requirement must be properly interpreted and translated into an established process, then continuously maintained. This results in a mix of required security practices and tools to monitor and enforce policies, while providing sufficient proof to support mandatory audits.

Our LogRhythm Labs compliance experts develop supporting content within our products to monitor your environment in strict ordinance with Payment Card Industry (PCI) Data Security Standard (DSS) regulatory controls. Because the Labs team updates content continually and enhances it to reflect the latest versions of PCI DSS, your team can avoid spending valuable time updating your compliance strategy. The content operates agnostic to underlying vendor network and security infrastructure.

LogRhythm's compliance content is easy to set up and vastly reduce ongoing maintenance. They further simplify future compliance needs by providing your organization with audit-ready alarms, reports, and dashboard views. For example, with predefined report packages aligned to the PCI DSS framework, you can significantly reduce the time it takes to demonstrate compliance with your auditor. These reports are organized to each specific control for easy identification and support during an audit to help simplify what can be a painstaking process.

> The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by credit card issuers to encourage and enhance cardholder data protection and facilitate the broad adoption of consistent data security measures globally. The PCI DSS applies to all organizations that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). Organizations provide proof during mandatory audits and adhering to strict reporting requirements on data breaches.

Penalties for Noncompliance

Every organization wants to avoid a breach, but when it comes to leaking credit card data, the stakes couldn't be higher. That is why a top reason businesses choose LogRhythm solutions is to address their PCI DSS compliance and avoid:

- Significant fines up to $500,000 per offense, plus $50–$90 per lost record
- Loss of revenue or being banned from accepting credit card payments
- Erosion of consumer confidence and severe reputation damage

Mature Beyond Meeting the Minimum Requirements

Don’t just monitor and report on compliance data, use LogRhythm’s capabilities to strengthen your security posture and actively protect sensitive data from evolving threats with case management, automation, and playbooks.

Tracking your incident response processes in case management reduces the amount of effort to meet with your PCI reporting requirements around compliance violations. Conveniently grant PCI auditors (QSAs) access to PCI-relevant cases where all the data and evidence is seamlessly collected and available for verification.

Compliance specific automations and playbooks enable you to rapidly update configuration settings, respond to policy violations, enforce protection controls, and more. With centralized visibility and command, you can proactively stop violations before they cause damage and make your next audit a breeze.

Benefits of Using LogRhythm for PCI DSS Compliance

Simplify Data Protection

With support for over 1,000 log source types, LogRhythm simplifies collection of your compliance data. Additionally, our Machine Data Intelligence (MDI) Fabric’s flexible data schema is source-type agnostic.

Reduce Management Overhead

Compliance content is continuously supported to evolving compliance controls and updates are delivered automatically. Leverage Success Services for even more support.

Expose Policy Violations

Advanced analytics use asset criticality data to generate accurate risk scores and effectively identify PCI policy violations as they occur. Dashboards and report packages provide access to the most critical compliance information at a glance.

Automate Policy Enforcement

LogRhythm offers guided workflows, customizable playbooks, and automation to optimize compliance efforts.

Extensive Data Support at Scale

LogRhythm's extensive support for both commercial and custom payment applications enable comprehensive monitoring of all information systems specified in both the PCI and Payment Application (PA) Data Security Standards. For easy identification, enterprise assets are mapped to each of the six control objective groups outlined in the table below.

PCI DSS Control Objectives & Requirements

Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.	LogRhythm monitors firewalls and network protection systems such as IDS/IPS and UTM, as well as behavior such as removing default passwords.
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.	LogRhythm monitors user behavior, configuration and file changes, and other types of activity that may jeopardize the protection or security of the cardholder.
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.	LogRhythm monitors anti-malware and vulnerability management products for threat exposure updates and can automatically kick off new scans.
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.	LogRhythm monitors access to cardholder systems and data. It alarms on the identification of policy violations and suspicious behavior.
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.	LogRhythm stores full audit trails and monitors access and network systems that perform regular tests to meet the conditions of these requirements.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.	LogRhythm supports monitoring information security policies and industry best practices, enabling organizations to meet PCI DSS.

To see how LogRhythm can mature your PCI DSS compliance strategy, schedule a demo.

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224 **www.logrhythm.com**