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 enforcing card companies require all organizations that store, process, or transmit cardholder data to be PCI compliant, providing proof during mandatory audits and adhering to strict reporting requirements on data breaches.

Eliminate Unnecessary Steps to Meet Compliance
Meeting to all the 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 developed this module to monitor your environment in strict ordinance with PCI DSS regulatory controls. Because the Labs team updates module content continually and enhances it to reflect the latest versions of PCI DSS, your team can avoid spending valuable time updating your compliance strategy. Module updates are automatically delivered, and they operate agnostic to underlying vendor network and security infrastructure.

LogRhythm's compliance automation modules are 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.

PCI MODULE AT A GLANCE
- 72 advanced analytics rules
- 29 lists defining “in-scope” content
- 89 saved searches to evaluate controls
- 6 defined reporting packages
- 98 summary reports provide oversight
- 95 detailed reports to assist audits

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 the top reason enterprises choose the LogRhythm NextGen SIEM Platform 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 SOAR solution to strengthen your security posture and actively protect sensitive data from evolving threats with Case Management, SmartResponse™ Automations, 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 900 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
Modules are continuously adapted to evolving compliance controls and updates are delivered automatically. Engage the Compliance Co-Pilot service 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’s SOAR solution offers guided workflows with customizable playbooks and automation to optimize the effort of responding to compliance alarms.

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

<table>
<thead>
<tr>
<th>Build and maintain a secure network</th>
<th>Protect cardholder data</th>
<th>Maintain a vulnerability management program</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect cardholder data.</td>
<td>3. Protect stored cardholder data.</td>
<td>5. Protect all systems against malware and regularly update antivirus software or programs.</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
<td>4. Encrypt transmission of cardholder data across open, public networks.</td>
<td>6. Develop and maintain secure systems and applications.</td>
</tr>
<tr>
<td>✓ LogRhythm monitors firewalls and network protection systems such as IDS/IPS and UTM, as well as behavior such as removing default passwords.</td>
<td>✓ LogRhythm monitors user behavior, configuration and file changes, and other types of activity that may jeopardize the protection or security of the cardholder.</td>
<td>✓ LogRhythm monitors anti-malware and vulnerability management products for threat exposure updates and can automatically kick off new scans.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement strong access control measures</th>
<th>Regularly monitor and test networks</th>
<th>Maintain an information security policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Restrict access to cardholder data by business need-to-know.</td>
<td>10. Track and monitor all access to network resources and cardholder data.</td>
<td>12. Maintain a policy that addresses information security for all personnel.</td>
</tr>
<tr>
<td>8. Identify and authenticate access to system components.</td>
<td>11. Regularly test security systems and processes.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data.</td>
<td>✓ LogRhythm stores full audit trails and monitors access and network systems that perform regular tests to meet the conditions of these requirements.</td>
<td>✓ LogRhythm supports monitoring information security policies and industry best practices, enabling organizations to meet PCI DSS.</td>
</tr>
<tr>
<td>✓ LogRhythm monitors access to cardholder systems and data. It alarms on the identification of policy violations and suspicious behavior.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Contact info@logrhythm.com for details on how LogRhythm can mature your PCI DSS compliance strategy, and ask us about the Compliance Co-Pilot Service.