The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements and industry best practices for preventing unauthorized access to cardholder data, including debit, credit, pre-paid, epurse, ATM, and point-of-sale (POS) card brands.

Complying with five of the PCI DSS requirements can be challenging because they require a combination of security tools, and threat management. This is where Alert Logic is uniquely positioned to help with a security platform, threat intelligence and experts:

- Protect all systems against malware
- Develop and maintain secure systems and applications
- Track and monitor all access to network resources and cardholder data
- Run vulnerability scans at least quarterly, and after any significant change in your network
- Implement an Incident Response Plan

Alert Logic will help you capture the right data, minimize storage requirements, so you can address these most challenging PCI requirements, and trace activity to gain a deeper understanding of what happened when an event occurs.

To Learn more about the Alert Logic Console and Reports, visit the Alert Logic documentation page.
PCI AUDIT REPORTING:

Alert Logic provides pre-built PCI audit reports to meet your PCI security and compliance requirements.

Alert Logic also provides saved views, and dashboards to meet many of your security and compliance requirements on day one. It's easy to correlate events and set automatic alerts and reporting to enable rapid response to security events.
Alert Logic collects, aggregates and normalizes log data whether it originates in your own data center, a hosted environment or the cloud. You get a unified view into all your data, with tools to rapidly uncover the insight and alerts you need to remain secure and compliant. Alert Logic provides hundreds of pre-built reports, saved views, and dashboards to meet many of your security and compliance requirements on day one. It’s easy to correlate events and set automatic alerts and reporting to enable rapid response to security events.

**LOG MANAGEMENT**

- Log Management Users
- Log Management Deployment
- Log Management Traffic
- Log Retention Settings
- Log Sources
- Log Search Stats
- Local Appliance Access Logs
- Appliance & Agent Health
- Notification Policies

**MALWARE PROTECTION**

- Automatically Gather New Malware and Goodware Samples
- Continuously Train Protection Models Against New Security Threats
- Tailor Protection Models Based on Organization Profile
- Maximize Protection and Minimize False Positives

The Alert Logic Console – Event Viewer will display the latest malware attempts to help you meet PCI requirement to protect against malware attacks.
VULNERABILITY MANAGEMENT

- INTERNAL SCAN SCHEDULE
- INTERNAL SCAN RESULTS
- PCI ASV SCAN SCHEDULE
- PCI ASV SCAN RESULTS
- NEW VULNERABILITY CHECKS
- CIS BENCHMARK SCAN RESULTS
- CONFIGURATION REMEDIATIONS
- SECURITY REMEDIATIONS
- TRI SCORES

Alert Logic is an approved PCI Scanning vendor. Through the Alert Logic console, you can schedule quarterly external scans that are required for PCI compliance.
Alert Logic uses colors and icons to help you easily identify the threat levels of exposures.

Alert Logic provides you with information about the exposure, including threat level, evidence, and recommendations to address the exposure.
# DETAILED SOLUTION MAPPING FOR PCI COMPLIANCE

<table>
<thead>
<tr>
<th>PCI</th>
<th>ALERT LOGIC MDR ESSENTIALS</th>
<th>ALERT LOGIC MDR PROFESSIONAL</th>
<th>ALERT LOGIC MDR ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 (a)(1)(i)(A) - Identify newly discovered security vulnerabilities</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>6.6 (a)(1)(i)(B) - Address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.1 (a)(1)(i)(D) - Implement audit trails to link all access to system components to each individual user</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.2 (a)(1)(i)(D) - Automated audit trails</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.3 (a)(1)(i)(D) - Caputre audit trails</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.5 (a)(1)(i)(D) - Secure logs</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.5.5 - Change detection to ensure integrity for log files</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.6 (a)(1)(i)(D) - Review logs at least daily</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.7 (a)(1)(i)(D) - Maintain logs online for three months</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>10.8.1 (a)(1)(i)(D) - Retain audit trails for at least one year</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>11.2 (a)(1)(i)(D) - Perform network vulnerability scans by an ASV at least quarterly or after any significant network change (Includes 11.2.1, 11.2.2, 11.2.3)</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>11.4 (a)(1)(i)(D) - Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the networks</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>11.5 - Change detection to ensure integrity for critical system files, configuration files, or content files</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>12.10.1 (a)(1)(i)(D) - Implement an incident response plan. Be prepared to respond immediately to a system breach</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

Using these capabilities, Alert Logic helps you to address the most challenging PCI DSS compliance requirements, so you get better outcomes across your entire compliance program.

**SAVE MONEY**
- Single Integrated Solution.
- Suite of Security Capabilities.
- One Monthly Subscription.

**STAFFING RELIEF**
- Our Experts are Included.
- 24/7 Threat Monitoring.
- 15-Min Live Notifications

**START FAST**
- Ready-to-Use Services.
- Expert Onboarding Assistance.
- Personal Tuning & Training.

---

© 2020 Alert Logic, Inc. All rights reserved. Alert Logic and the Alert Logic logo are trademarks, registered trademarks, or servicemarks of Alert Logic, Inc. All other trademarks listed in this document are the property of their respective owners.