



LogLogic Compliance Suite: PCI Edition

Automate Reports & Alerts. Accelerate Time to Compliance.

The LogLogic Compliance Suite for the Payment Card Industry (PCI) Data Security Standard is the first solution of its kind. It instantly turns log data into automated reports and alerts for monitoring PCI controls and requirements. IT Directors and organizations interacting with credit card data can reduce the cost of compliance, improve time to remediation and mitigate risk.

Whether you are buying books online or groceries at a local store, virtually every computer-based transaction results in a log data file that is a fingerprint of user and systems activity. LogLogic makes the billions of log messages generated by retailers and merchants using credit cards available for enforcing, auditing and automating the requirements and controls related to the Payment Card Industry (PCI) Data Security Standard. The second of LogLogic's Compliance Suites, the PCI Edition delivers more than 80 customizable PCI reports and alerts.

The PCI Data Security Standard was established to restore consumer confidence in card payments, and is intended to protect the environments that store, process or transmit credit card data. Merchants must comply with the standard or face substantial fines or be barred from the card acceptance program. PCI compliance applies to any organization that stores, processes or transmits cardholder data. Therefore, this standard applies to not only store merchants, but banks, service providers and card processors. In addition, the security requirements extend to all "system components" such as servers, applications, and any network component (eg. firewalls, switchers, routers) included in, or connected to, the cardholder data environment.

The LogLogic Compliance Suite: PCI Edition delivers automated process validation, reporting and alerts based on log data to evidence and enforce PCI compliance. The Compliance Suite removes the complexity and resource requirements of PCI compliance efforts. LogLogic's award-winning appliances are designed to collect and store log data in accordance with the PCI Data Security Standard. Combining LogLogic's appliances and the Compliance Suite: PCI Edition, IT Administrators, merchants, auditors and financial executives can reduce time to compliance and realize dramatic improvements in risk mitigation and audit accuracy.

Extensive Benefits. Rapid ROI.

With LogLogic's Compliance Suite, IT personnel can reduce the development and management of audits and reporting from weeks to an hour or less. Enterprises can achieve sustainable compliance with a fraction of the resources or risks of alternate solutions.

- Time reduction of up to two weeks per report and dramatic improvement in risk mitigation.
- ROI of 1 to 3 months based on reduced consulting, personnel and infrastructure costs.
- Sustainable compliance and a significant reduction in risk by delivering real-time, automated alerting on PCI policies.

Key Features and Benefits

- Automates PCI compliance activities and dramatically improves audit accuracy.
- Accelerates time to risk mitigation.
- Allows organizations to use infrastructure data to provide evidence of, and enforce, IT controls.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting for PCI compliance.
- Delivers over 80 out-of-the-box compliance reports and over 30 out-of-the-box alerts.
- Enables customization of any Compliance Report using LogLogic's Agile Reporting Engine to map reports against your company's policies.

Over 80 Reports. Over 30 Alerts.

The LogLogic Compliance Suite is the first solution to provide out-of-the-box validation of PCI using log data. Log data allows organizations to manage the extreme challenges of meeting major PCI DSS requirements. LogLogic's compliance reports and alerts generally fall into the following categories:

- **Security.** Reports and alerts show that all network security devices, including firewalls and IDS systems, have been configured appropriately to allow only the requested and approved traffic in and out of the network.
- **Change Management.** Reports and alerts show that all systems and system changes are appropriately requested, approved, tested, and validated by authorized personnel prior to implementation to the production environment.
- **Identity and Access.** Reports and alerts show that all PCI-related systems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data, and that a division of roles and responsibilities have been implemented to reduce the possibility for a single individual to subvert a critical process.
- **Monitoring and Reporting.** Reports and alerts to allow customers to continuously monitor the IT infrastructure for any security violations.

The LogLogic Compliance Suite: PCI Edition focuses on key requirements to regularly monitor all access to network resources and cardholder data (Requirement #10 of the PCI DSS). This includes establishing automated audit trails to reconstruct events, such as invalid access attempts, actions taken by individuals, creation and deletion of system-level objects and others. Additionally, it focuses on securing audit trails so that they cannot be altered, including limiting views, protecting them from unauthorized modifications, promptly backing them up, and establishing copies, among others.

Key Features and Benefits

Agile Log Reporting

Create highly customized reports from easy-to-use templates. Create reports for PCI in seconds with no vendor intervention.

Log Learning

Powerful artificial intelligence and machine learning lets administrators set alerts based on changes to individual devices, groups of devices or the network.

Log Forensics

Indexing and "Google-like" search algorithms allow near-instant data retrieval – search terabytes of unaltered, unfiltered data in seconds.

Open Log Routing

Routes raw data, reports and alerts to existing SIEM, network management, and trouble ticket/ other solutions.

Log Process Audit

Enables network activity audits to provide proof of compliance or critical information for legal proceedings.

Requirements Addressed by LogLogic for PCI DSS

Category	PCI Data Security Standard	
Security	Requirement 1	Install and maintain a firewall configuration to protect data
	Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
	Requirement 11	Regularly test security systems and processes
Change Management	Requirement 6	Develop and maintain secure systems and applications
Identity and Access	Requirement 7	Restrict access to data by business need-to-know
	Requirement 8	Assign a unique ID to each person with computer access
Monitoring and Reporting	Requirement 10	Track and monitor all access to network resources and cardholder data

More information

Visit www.loglogic.com or contact a LogLogic representative by e-mail: info@loglogic.com, or phone: 1.888.347.3883

LogLogic is a registered trademark in the USA and/or other countries. All other brand names, product names, or trademarks belong to their respective holders. LogLogic reserves the right to alter product offerings and specifications at any time without notice, and is not responsible for typographical or graphical errors that may appear in this document.

© 2009 LogLogic, Inc. All rights reserved.

