ManageEngine
Log360

How SIEM helps businesses comply with the PCI DSS

www.manageengine.com/log-management/

The Payment Card Industry Data Security Standard (PCI DSS) framework is critical to organizations handling credit card transactions. Established by the Payment Card Industry Security Standards Council—which includes major payment brands such as American Express, Discover, JCB International, MasterCard, and Visa—the PCI DSS establishes the baseline for securing payment card data.

This standard has evolved to address emerging threats and technological advancements since its initial release in 2004. The latest iteration, PCI DSS v4.0, introduced in March 2022, reflects feedback from over 200 organizations and incorporates over 6,000 suggestions to remain relevant in the complex and fast-changing payment security landscape.

Version 4.0 introduces new requirements and refines existing ones, expanding the scope of data security coverage. These changes enhance security controls, clarify guidelines, and offer greater flexibility in implementing and validating security measures. This evolution signifies a shift towards an adaptive, continuous security approach, addressing the dynamic nature of cyber threats and underscoring the necessity for up-to-date, robust defenses in the payment card industry.

Compliance with PCI DSS involves adhering to twelve key requirements that focus on continuous improvement through regular assessments, repair, and reporting. This guide will delve into how the advanced capabilities of security information and event management (SIEM) solutions align with and support compliance with these updated requirements of PCI DSS.

The role of SIEM in PCI DSS compliance

Achieving and maintaining compliance with PCI DSS 4.0 is critical for organizations handling cardholder data. The increasing challenges in safeguarding sensitive information can be overcome with a SIEM solution. These solutions offer a multifaceted approach to addressing various PCI DSS requirements, particularly important for medium and large-sized organizations.

For example, a SIEM solution is adept at monitoring,alerting, and logging events required by network security controls (PCI DSS IDs 1.2, 1.3), making it easier to monitor and restrict network access to and from the cardholder data environment and to monitor changes to critical network configurations. This capability is crucial in preventing unauthorized access. The management of network connections between trusted and untrusted networks (1.4) is another area where SIEM provides invaluable support. It achieves this through the timely detection of and response to potential security threats by identifying malicious traffic.

Regarding anti-malware and anti-phishing mechanisms (5.2, 5.3, 5.4), SIEM solutions improve security by integrating with anti-malware tools and threat feeds. This integration enhances an organization's ability to detect, alert on, and respond to malware and phishing attacks.

A standout feature of SIEM solutions is their capability in comprehensive audit logging (10.2). They implement extensive logging across various systems and applications, supporting anomaly detection and suspicious activity monitoring. This aids in forensic analysis and ensures that all actions within the network are traceable and accountable, aligning with the fundamental requirements of PCI DSS. Audit logs are also protected from unauthorized modifications (10.3), and alerts are configured to identify suspicious activities (10.4). This level of vigilance is vital in securing the organization against threats that can emerge from any vector at any time.

In addition, SIEM solutions support the detection of and response to network intrusions and unexpected file changes (11.5), offering an additional layer of security through file integrity monitoring.

Therefore, a SIEM solutions is essential for meeting the demands of PCI DSS v4.0. Their comprehensive features, including logging, real-time monitoring, and network security, perfectly match the rigorous standards set by the PCI DSS. SIEM is a core component for any organization committed to protecting their cardholder data environment in the rapidly evolving cyber threat landscape.

PCI DSS requirements fulfilled by ManageEngine Log360

PCI DSS ID	Defined approach requirements	How Log360 helps
1.2 Network security controls (NSCs) are configured and maintained.		
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined in at Requirement 6.5.1.	Log360 monitors and audits all network activities and configuration changes. The configuration change monitoring ensures all changes are logged, providing an audit trail for review and approval as required by change control processes.
1.2.8	Configuration files for NSCs are: Secured from unauthorized access and, Kkept consistent with active network configurations.	Log360's File Integrity Monitoring (FIM) add-on secures NSC configuration files against unauthorized access. It tracks changes to these files, ensuring they align with active configurations.
1.3 Network access to and from the cardholder data environment is restricted.		
1.3.1	Inbound traffic to the CDE is restricted as follows: To only traffic that is necessary., All other traffic is specifically denied.	Log360's real-time monitoring helps with ensuring necessary traffic is allowed. Unnecessary or suspicious inbound network traffic can be instantly flagged and investigated.
1.3.2	Outbound traffic from the CDE is restricted as follows: To only traffic that is necessary., All other traffic is specifically denied.	Similar to inbound traffic monitoring, Log360 can track outbound traffic from the CDE, allowing only necessary communications and flagging any unauthorized or unexpected traffic patterns for investigation.

1.4 Network connections between trusted and untrusted networks are controlled.		
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks.	While Log360 does not control access, it can monitor and audit network connections to ensure that systems storing cardholder data are not accessed from untrusted networks.
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	Log360's auditing capabilities include detecting and alerting on unauthorized disclosure of internal IP addresses and routing information.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks and the CDE as follows: Specific configuration settings, Security controls actively running, Security controls not alterable by users.	Log360 can monitor and report on the security posture of devices, ensuring compliance with required security controls.
2.2 System components are configured and managed securely.		
2.2.2	Vendor default accounts are managed as follows: If used, the default password is changed per Requirement 8.3.6, If not used, the account is removed or disabled.	Log360 can track and report on user account changes, including vendor default accounts, ensuring compliance with password and account management policies.
2.3 Wireless environments are configured and managed securely.		
2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or confirmed to be secure, including but not limited to: Default wireless encryption keys, Passwords on wireless access points, SNMP defaults.	Log360 can audit changes in wireless network configurations, ensuring all default settings are secure and compliant with PCI DSS requirements.
2.3.2	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as needed.	Log360 can monitor and report on changes to wireless encryption keys, ensuring they are updated in compliance with PCI DSS requirements.
3.4 Access to displays of full PAN(primary account number) and ability to copy PAN is restricted.		
3.4.2	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	Log360 doesn't directly control access to PAN data but can monitor and alert on unauthorized access or copying of PAN, especially through remote-access technologies.

5.2 Malicious software (malware) is prevented, or detected and addressed.		
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	Log360 helps in identifying which system components are at risk from malware through continuous monitoring and log analysis, supporting periodic evaluations required by this clause.
5.2.2	The deployed anti-malware solution(s) detects all known types of malware, and removes, blocks, or contains all known types of malware.	Log360 aids in the detection process by providing detailed logs and alerts for any activity that could be related to malware, thus enhancing the effectiveness of deployed anti-malware solutions.
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	While Log360 does not directly update anti-malware solutions, it can monitor and log the update status of these solutions, ensuring they are current and effective.
5.3.2	The anti-malware solution(s) performs periodic scans and active or real-time scans, OR performs continuous behavioral analysis of systems or processes.	Log360 supports the monitoring of anti-malware activities, including periodic and real-time scans, through its log management capabilities.
5.3.3	For removable electronic media, the anti-malware solution(s) performs automatic scans or continuous behavioral analysis when the media is inserted, connected, or logically mounted.	Log360 can track and log activities related to removable media, aiding in the enforcement of anti-malware scans.
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Log360 can collect, retain, and manage audit logs from various anti-malware solutions, ensuring compliance with Requirement 10.5.1.
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	Log360's alerting system can notify administrators if anti-malware solutions are altered or disabled, helping enforce this requirement.
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	With its auditing features for Microsoft 365 and Exchange Server, Log360 ensures that phishing attempts are effectively identified and stopped. It monitors, analyzes, and alerts on malicious attachments by analyzing both inbound and outbound email traffic.

6.3 Security vulnerabilities are identified and addressed.		
6.3.1	Security vulnerabilities are identified and managed using industry-recognized sources, assigned a risk ranking, covering vulnerabilities for bespoke and custom, and third-party software.	Log360, through its integration with vulnerability scanners, can assist in identifying and managing security vulnerabilities, providing logs and reports for compliance.
6.4 Public-facing web applications are protected against attacks.		
6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis, protected against known attacks through reviews or automated technical solutions.	Log360 can monitor and log web server and application activities, aiding in the detection of threats and vulnerabilities to public-facing web applications.
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, generating audit logs and configured to either block attacks or generate an alert for investigation.	Log360's real-time monitoring and alerting capabilities can help detect web-based attacks against public-facing applications.
7.2 Access to system components and data is appropriately defined and assigned.		
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed periodically to ensure they remain appropriate, with any inappropriate access addressed.	Log360 can regularly review and report on user account privileges and ensure they remain as configured.
7.2.5.1	All access by application and system accounts and related access privileges are reviewed periodically, with any inappropriate access addressed, and management acknowledges that access remains appropriate.	Log360 can also review and report on application and system account access, helping ensure compliance with this requirement.
7.2.6	User access to query repositories of stored cardholder data is restricted, with direct unfiltered query access prohibited, unless performed by an authorized administrator.	Log360 can monitor and audit database queries, ensuring restricted access to stored cardholder data.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		
8.2.5	Access for terminated users is immediately revoked.	Log360 monitors and reports on user account statuses to ensure timely access revocation for terminated users.
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	Log360 can identify and report on inactive user accounts, aiding in their timely removal or disabling.

8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: Enabled only during the time period needed and disabled when not in use, Use is monitored for unexpected activity.	Log360 can monitor and manage third-party account usage, ensuring these accounts are enabled only when needed and disabled otherwise.
8.3 Strong authentication for users and administrators is established and managed.		
8.3.4	Invalid authentication attempts are limited by: Locking out the user ID after not more than 10 attempts, Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	Log360 tracks and reports on failed logon attempts. It can alert administrators when the threshold for failed attempts is exceeded thereby aiding compliance with user ID lockout policies.
8.3.5	If passwords/passphrases are used as authentication factors, they are set and reset for each user as follows: Set to a unique value for first-time use and upon reset, Forced to be changed immediately after the first use.	While Log360 does not directly manage password resets, it monitors and reports on password reset activities and policy changes in the Active Directory environment.
8.3.6	If passwords/passphrases are used as authentication factors, they meet the following minimum level of complexity: A minimum length of 12 characters (or eight characters if the system does not support 12), Contain both numeric and alphabetic characters.	Log360 doesn't enforce password complexity directly but can report on password policy changes in Active Directory, helping ensure compliance with complexity requirements.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	Log360 collects and stores audit logs from various sources, ensuring that audit logs are continuously active and available for all system components and cardholder data.
10.2.1.1	Audit logs capture all individual user access to cardholder data.	Log360 captures detailed logs that include user access to cardholder data by helping meet the requirement of monitoring and capturing individual user activities.
10.2.1.2	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Log360 specifically monitors and logs all administrative activities, including system changes and data access, ensuring comprehensive logging of all critical actions.
10.2.1.3	Audit logs capture all access to audit logs.	Log360 ensures that all access to its own audit logs is monitored and recorded, complying with the requirement of logging access to audit logs.

10.2.1.4	Audit logs capture all invalid logical access attempts.	Log360 records all invalid access attempts, providing detailed insights into such events for security analysis.
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including: Creation of new accounts, Elevation of privileges, Changes to accounts with administrative access.	Log360 can log and alert on changes to identification and authentication credentials, including account creation and privilege elevation.
10.2.1.6	Audit logs capture: All initialization of new audit logs, All starting, stopping, or pausing of existing audit logs.	Log360 ensures that events such as the initialization or modification of audit logs are captured and reported.
10.2.1.7	Audit logs capture all creation and deletion of system-level objects.	Log360 tracks and logs the creation and deletion of system-level objects, providing necessary audit trails for compliance.
10.2.2	Audit logs record details for each auditable event: User identification, Type of event, Date and time, Success and failure indication, Origination of event, Identity or name of affected data, system component, resource, or service.	Log360 captures comprehensive details of auditable events, including user identification, event type,date and time, and success and failure indications.
10.3 Audit logs are protected from destruction and unauthorized modifications.		
10.3.1	Read access to audit logs files is limited to those with a job-related need.	Log360 restricts access to audit logs through role-based access control, ensuring that only authorized personnel can view the logs, in line with job-related requirements.
10.3.2	Audit log files are protected to prevent modifications by individuals.	Log360's secure storage and restricted access prevent unauthorized modifications to audit log files. It also maintains a clear audit trail of any access or changes to the logs.
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	Log360 facilitates prompt backup of log files to a secure, centralized server. This ensures that logs from various sources, including external-facing technologies, are safely archived and protected.
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	Log360 employs file integrity monitoring and change-detection mechanisms, alerting administrators to any unauthorized changes to log files, ensuring the integrity of log data.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		
10.4.1	The following audit logs are reviewed at least once daily: All security events, Logs of all system components that store, process, or transmit CHD and/or SAD, Logs of all critical system components, Logs of all servers and system components that perform security functions.	Log360's automated log collection and analysis features facilitate daily reviews of all required audit logs. It can generate reports and alerts based on specific criteria, such as security events and actions on critical components.
10.4.1.1	Automated mechanisms are used to perform audit log reviews.	Log360 automates the process of audit log reviews with its advanced analytics and reporting capabilities, ensuring continuous monitoring and timely detection of any security incidents or policy violations.
10.4.2	Logs of all other system components are reviewed periodically.	Log360's automated log reporting allows for regular and systematic examination of logs from various system components, aligning with periodic review requirements.
10.4.2.1	The frequency of periodic log reviews for all other system components is defined in the entity's targeted risk analysis.	Log360 allows customization of log reporting schedules, enabling organizations to define frequencies based on their risk analysis and compliance requirements.
10.4.3	Exceptions and anomalies identified during the review process are addressed.	Log360's advanced analytics and alerting mechanisms help in identifying and addressing exceptions and anomalies during log reviews, ensuring prompt response to potential issues.
10.5 Audit log history is retained and available for analysis.		
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Log360's log retention settings can be configured to retain logs for 12 months or more, with immediate access to the most recent three months, aiding in efficient analysis and compliance.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		
10.6.1	System clocks and time are synchronized using time-synchronization technology.	Log360 relies on the underlying system's time synchronization but ensures that all log data is consistently timestamped based on the system time for accurate event tracking.
10.6.3	Time synchronization settings and data are protected as follows: Access to time data is restricted to only personnel with a business need, Any changes to time settings on critical systems are logged, monitored, and reviewed.	Log360 can monitor and log any changes to system time settings, ensuring that time synchronization data and settings are secure and auditable.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
10.7.1	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: Network security controls, IDS/IPS, FIM, Anti-malware solutions, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used).	Log360 can be configured to monitor and alert on failures of various security controls, ensuring rapid detection and response to any issues with these systems.
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: Network security controls, IDS/IPS, Change-detection mechanisms, Anti-malware solutions, Physical access controls, Logical access controls, Audit logging mechanisms, Segmentation controls (if used), Audit log review mechanisms, Automated security testing tools (if used).	With Log360, administrators receive immediate alerts on failures of critical security controls, enabling swift action to address and mitigate risks.
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: Restoring security functions, Identifying and documenting the duration of the security failure, Identifying and documenting the cause(s) of failure and required remediation, Determining whether further actions are required as a result of the security failure, Implementing controls to prevent the cause of failure from reoccurring, Resuming monitoring of security controls.	Log360 supports rapid response mechanisms through its alerting and reporting features, which help in quickly addressing failures of security controls.
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
11.2.1	Authorized and unauthorized wireless access points are managed as follows: The presence of wireless (Wi-Fi) access points is tested for, All authorized and unauthorized wireless access points are detected and identified, Testing, detection, and identification occurs at least once every three months.	Through integration with network monitoring tools, Log360 can assist in the detection and logging of both authorized and unauthorized wireless access points.

11.5 Network intrusions and unexpected file changes are detected and responded to.		
11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: All traffic is monitored at the perimeter of the CDE, All traffic is monitored at critical points in the CDE, Personnel are alerted to suspected compromises, All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Log360 utilizes advanced intrusion detection/prevention techniques to monitor traffic at CDE perimeters and critical points, alerting personnel to suspected compromises. It also ensures that detection engines and signatures are updated.
11.5.1.1	Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	Log360's intrusion detection capabilities can identify and alert on covert malware communication channels, enhancing network security against sophisticated threats.
11.5.2	A change-detection mechanism is deployed as follows: To alert personnel to unauthorized modification of critical files, To perform critical file comparisons at least once weekly.	Log360's change-detection mechanism alerts personnel to unauthorized modifications of critical files and performs file comparisons at least weekly, aiding in compliance with this requirement.
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.		
A1.2.2	Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.	Log360 facilitates forensic investigations through its comprehensive incident management module. This helps with the prompt investigation of security incidents for any customer.
A1.2.3	Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: Customers can securely report security incidents and vulnerabilities to the provider, The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	Log360 supports mechanisms for reporting and addressing security incidents and vulnerabilities, including secure reporting channels for customers and prompt remediation in line with Requirement 6.3.1.
A3.5 Suspicious events are identified and responded to.		
A3.5.1	A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: Identification of anomalies or suspicious activity as it occurs, Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel, Response to alerts in accordance with documented response procedures. PCI DSS Reference: Requirements 10, 12	Log360 implements methodologies for identifying anomalies or suspicious activities in real-time, issuing prompt alerts, and facilitating a documented response procedure in line with PCI DSS requirements.

Integrating PCI DSS compliance within the broader scope of IT security is essential, not just advisable. This process requires a detailed evaluation of current security protocols and the implementation of robust strategies to address any security vulnerabilities. Log360 can redefine an organization's compliance posture through embedding continuous, automated, and intelligent security practices into the core of organizational IT infrastructure.

Log360 leads this transformation with its advanced features in real-time log management and IT compliance. It provides a user-friendly, all-encompassing solution for centralized logging, real-time monitoring, and threat detection by promoting a proactive approach to cyber threats. Log360 simplifies the compliance journey by automating PCI DSS report generation. The integration with threat intelligence feeds is particularly beneficial as it allows for real-time updates on emerging security threats. This feature ensures that an organization's security protocols and compliance efforts are consistently aligned with the latest threat landscape, reducing the complexity and effort required to maintain PCI DSS compliance.

We encourage you to discover the benefits of Log360 for yourself with a free, fully functional, 30-day trial.

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

↓ Download