ManageEngine
DataSecurity Plus

PCI-DSS Compliance

Achieving PCI DSS compliance using DataSecurity Plus

Achieving PCI DSS compliance using DataSecurity Plus

The Payment Card Industry Data Security Standard (PCI DSS) applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. It also applies to other entities that accept, store, or transmit payment card information, cardholder data, or sensitive authentication data (SAD).

ManageEngine DataSecurity Plus, our PCI compliance software, helps address the requirements of the PCI DSS by:

- Discovering and reporting on payment card information in storage environments.
- Auditing how sensitive files are secured, processed, and transmitted.
- Monitoring file integrity in the cardholder data environment (CDE).
- Providing enhanced insights into security permissions and file storage.
- Protecting sensitive files from accidental or malicious data leaks.
- And doing much more.

How our PCI DSS compliance software helps address PCI compliance requirements

What the PCI DSS requirements are	What you should do	How DataSecurity Plus helps you
Requirement 2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functions are removed or disabled.	Identify all system functions, such as scripts, file systems, and unnecessary web servers, and remove the ones that are not in use.	**Analysis of unused files** Receive reports on files, scripts, and batch files that have not been accessed or modified for extended periods of time.
Requirement 3.2.1 Account data storage is kept to a minimum through the implementation of data retention and disposal policies as follows: • Coverage for all locations of stored account data • Coverage for any SAD • Limits on the data storage amount and retention time to what is required for legal, regulation, or business requirements • Specific retention requirements for stored account data that defines the length of the retention period • Processes for securely deleting or rendering unrecoverable the account data when it is no longer needed according to the retention policy • A process for verifying, at least once every three months, that the stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable	Periodically scan for regulated data in your CDE. Set up data retention policies and delete collected data when it is no longer needed. Locate and remove cardholder data that is stored beyond its permissible lifetime.	**PCI and cardholder data discovery** Use built-in data discovery rules to locate PCI and cardholder data stored by your organization. Create an inventory of what data is stored, where, by whom, and for how long. **Analysis of redundant, obsolete, and trivial data** Identify old, stale, and unmodified files to ensure that cardholder data is not stored beyond its intended retention period. **Scheduled data risk assessment scans** Perform periodic cardholder data discovery scans, enable incremental scanning of new and recently modified files, and ensure that every instance of regulated data is discovered and cataloged. You can also use file management options in the UI as well as custom scripts to quarantine or delete files that violate sensitive data storage policies.

Requirement 3.3 SAD is not stored after authorization. **Note:** This requirement does not apply to issuers and companies that support issuing services and have a business justification to store SAD. **Note:** SAD includes cardholder names, primary account numbers (PANs), card verification codes, personal identification numbers (PINs), and track data.	Examine data sources and verify that SAD is not stored after authorization.	**PCI data discovery** Implement effective data discovery with a combination of keyword-matching and pattern-matching. Together, these will help you locate card verification values, PINs, PANs, and other authentication data. **Confidence scoring** Verify the context of potential matches to determine the certainty of a match and reduce false positives. **Response automation** Automate the deletion or quarantining of detected card data or limit its use by carrying out a customized action using scripts.
Requirement 3.4.2 Prevent the copying and/or relocation of PANs for all personnel, except for those with authorization.	Prohibit users from storing or copying files containing cardholder data onto their local personal computers or other media.	**Clipboard control** Enable granular control by auditing and blocking copy actions triggered on local devices and in the organizational network. **USB write protection** Blocklist suspicious USB devices and prevent users from exfiltrating sensitive data.
Requirement 3.5.1 PANs are rendered unreadable anywhere they are stored, and cleartext PANs are removed.	Identify and remove cleartext PANs stored on your storage media.	**Management of files containing sensitive data** Move or delete files containing sensitive data as a risk mitigation action.
Requirement 3.6.1 Access to cryptographic keys is restricted to the smallest number of custodians necessary.	Examine the permissions associated with sensitive files and ensure that access is restricted to the smallest number of users.	**NTFS and share permission reporting** Receive detailed reports on the NTFS and share permissions of files and folders to know which users have what permissions to them.

Requirement 6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and the documentation is updated as applicable.	Protect your systems with file integrity monitoring (FIM) software to examine critical files for changes made to their content and metadata.	**File change monitoring** Track accidental, inappropriate, and unauthorized changes by monitoring all file activities, including permission changes as well as file creations, modifications, and deletions.
Requirement 7.2.1 An access control model is defined and granted as follows: • Appropriate access depending on the entity's business and access needs • Access to system components and data resources based on the user's job classification and function • The least privileges required (for example, user or administrator privileges) to perform a job function **Note:** System components include network devices, servers, computing devices, and applications.	Verify that the privileges assigned to privileged and non-privileged users are: • Necessary for each individual's job function. • Restricted to the least privileges necessary to perform job responsibilities.	**Effective permission analysis** Ensure the confidentiality of cardholder data by analyzing and reporting on effective permissions. Verify that each user does not have more privileges than required for their role. **Detection of overexposed files** Locate files that can be accessed by every employee as well as files that allow Full Control access for users.
Requirement 7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months • To ensure user accounts and access remain appropriate based on job function • To address any inappropriate access • With management verifying that the access remains appropriate	Review privileged user accounts periodically to make sure that the implemented access control measures are appropriate.	**Scheduled reporting** Set up automatic, periodic reports on privileged users and inactive users. These reports can be emailed on a set schedule to multiple stakeholders. **Security permission analysis** Track permission changes, list effective permissions, identify files that can be accessed by every employee, find users with Full Control privileges, and do even more to ensure that the principle of least privilege is followed.

Requirement 7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application • With access being limited to the systems, applications, or processes that specifically require that access	Make sure access rights to application and system accounts are limited to what is required.	**NTFS permission reporting** List users who have access to files containing cardholder data and include details on which actions each user can perform on them.
Requirement 8.2.5 Access for terminated users is immediately revoked.	Ensure that users who are terminated from your organization are removed from file access lists.	**File ownership analysis** Identify orphaned files and files owned by stale, disabled, or inactive users to prevent malicious file change attempts by terminated employees.
Requirement 10.2.1 Audit logs are enabled for all system components and cardholder data to link all access attempts to individual users. Capture all successful and failed access attempts by all users, including ones with root or administrative privileges.	Collect detailed logs on user activity in your CDE. Track changes made by users with administrative privileges.	**Detailed audit trails** Track critical file access attempts, web app usage, USB usage, printer usage, and more with a centralized access audit log. **Privileged user monitoring** List users with privileged access to sensitive files and customize reports to monitor all the file changes they make.
Requirement 10.2.2 Record the following details for each auditable event: • User identification • The type of event • The date and time • The success or failure indication • The origination of the event • The identity or name of the affected data, system component, resource, or service (for example, the name and protocol)	Generate audit logs that provide the ability to trace suspicious activity back to a specific user. Audit user activity in your CDE in real time.	**Root cause analysis** Leverage granular report filtering options to expedite root cause analysis and identify the extent of a breach. **Real-time change auditing** Get complete information on every file access attempt, including details on who attempted what change, in which file, when, from where, and whether they were successful.

Requirement 10.3 Audit logs are protected from destruction and unauthorized modifications. Use FIM or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Implement FIM or change detection software to check for changes to critical files and send notifications when such changes are noted.	**PCI FIM** Audit every successful and failed file access attempt in real time. Maintain a detailed audit trail for analysis. **Real-time alerts** Trigger instant alerts to notify stakeholders when suspicious file changes are detected. **Automated security incident responses** Execute automated responses to minimize the potential damage of a security incident.
Requirement 10.4 Audit logs are reviewed to identify anomalies or suspicious activity.	Use automated mechanisms to review logs periodically in order to identify potential issues and reduce the time it takes to detect a potential breach.	**Scheduled delivery of PCI** compliance reports Deliver scheduled reports to stakeholders' mailboxes in PDF, HTML, CSV, or XLSX format.
Requirement 10.5 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis (for example, online, archived, or restorable from a backup).	Retain logs for at least a year so that investigators have a sufficient log history to determine the length of a potential breach and its impact.	**Long-term audit log retention** Retain audit data for long periods. You can also archive older logs and reload them at a later date to analyze file access attempts.
Requirement 11.5.2 A change-detection mechanism (for example, a FIM tool) is deployed as follows: • Alert personnel to unauthorized modifications (including changes, additions, and deletions) of critical files. • Perform critical file comparisons at least once a week.	Monitor changes in system executables, application executables, configuration and parameter files, and more. Trigger alerts in the event of unexpected changes.	**FIM** Audit changes made to application- and OS-critical binaries, configuration files, application files, log files, and more. **Instant alerts** Notify administrators instantly when anomalous file changes are detected. **Custom incident responses** Automate batch files to shut down machines, end user sessions, and do even more.

• Implement a process to respond to any alerts generated by the change detection solution.		
Requirement A3.2.5.1 A data discovery methodology is implemented and confirmed as follows: • Ensure your methods are able to discover cleartext PANs in all types of system components and file formats in use. • Confirm the effectiveness of data discovery methods at least once every 12 months.	Periodically report on the locations of cardholder data in your file storage environment. Identify sensitive data residing outside your defined CDE.	**Multi-platform visibility** Detect sensitive cardholder and PCI data across Windows file servers, failover clusters, and Microsoft SQL Server databases. **Schedule-based PCI data discovery** Discover PCI data periodically and incrementally.
Requirement A3.2.5.2 Response procedures are implemented to be initiated upon the detection of cleartext PANs outside the CDE to include: • Determining what to do if cleartext PANs are discovered outside the CDE, including retrieving, securely deleting, and/or migrating them into the currently defined CDE, as applicable. • Determining how the data ended up outside the CDE. • Remediating data leaks or process gaps that resulted in the data being outside the CDE. • Identifying the source of the data. • Identifying whether any track data is stored with the PANs.	Perform remedial actions when sensitive data is discovered outside the CDE.	**Automated remediation** Automatically delete, move, or otherwise manage sensitive data when it is found outside the CDE. **Ownership and access analysis** Find out who owns the sensitive data and trace all user actions in the time frame under analysis. This will help you determine how the data ended up outside the CDE.

Requirement A3.2.6 Mechanisms are implemented to detect cleartext PANs leaving the CDE and prevent them from doing so via an unauthorized channel, method, or process, including the generation of audit logs and alerts upon the detection of cleartext PANs leaving the CDE. Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PANs from the CDE via an unauthorized channel, method, or process.	Implement data loss prevention solutions to detect and prevent leaks via emails, removable media, and printers.	**A unified data leak prevention platform** Classify sensitive files and prevent their leakage via external storage devices, Outlook, and printers. **Peripheral device usage control** Restrict the use of USB devices, wireless access points, and CD and DVD drives using central device control policies to protect against data exfiltration.
Requirement A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems—for example, using centrally managed or automated log correlation tools—to include at least the following: • The identification of anomalies or suspicious activities as they occur • The prompt issuance of alerts to the responsible personnel upon the detection of suspicious activities or anomalies • Responses to alerts in accordance with documented response procedures	Set up a solution that can identify undesirable events—such as critical file changes and intrusions—and notify administrators instantly.	**Anomaly detection** Identify user activity anomalies such as file access attempts after business hours or an excessive number of failed access attempts. **Rapid alerts** Configure alerts for unwarranted changes in critical files, the discovery of sensitive data outside the CDE, and more. **Threat detection and response** Detect ransomware intrusions and execute scripts for quarantining infected machines and preventing the spread of malware.

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore DataSecurity Plus' capabilities

File server auditing
Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis
Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment
Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention
Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection
Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more