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.

ManageEngine DataSecurity Plus — our PCI compliance software — helps address the requirements of 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 card data environment.
- Providing enhanced insights into security permissions and file storage.
- Protecting sensitive files from accidental and malicious data leaks.

And much more.

How our PCI DSS compliance software helps address PCI compliance requirements

This table lists the various requirements of the PCI DSS that are addressed by DataSecurity Plus.

What the PCI requirements are	What you should do	How DataSecurity Plus helps you
Requirement 2.2.5 Remove all unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	• Identify all system components including scripts and file systems, and remove the ones that are not in use.	**Locate unused files:** Receive reports on files, scripts, batch files, and more that have not been accessed or modified for extended periods of time. These reports simplify redundant, outdated, and trivial (ROT) file management and reduce the number of vulnerable files with outdated permissions or data.
Requirement 3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures, and processes that include at least the following for all cardholder data storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention	• Periodically scan for regulated data in your card data environment (CDE). • Set up data retention policies—collected data should be deleted when it is no longer needed. • Locate and remove cardholder data that is stored beyond its permissible life time.	**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. This allows administrators to ensure that only necessary data is stored. **ROT data analysis** 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 scripts to quarantine or delete files that violate sensitive data storage policies.

Requirement 3.2 Do not store sensitive authentication data after authorization. Sensitive authentication data includes cardholder name, primary account number (PAN), card verification code, personal identification number (PIN), and more. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business ustification • And the data is stored securely	Examine data sources and verify that sensitive authentication data 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 (CVV), PIN, PAN, and other authentication data. **Confidence scoring** Verify the context of potential matches to determine the certainty of a match being a True Positive instead of a False Positive. **Response automation** Automate the deletion or quarantining of detected card data, or limit its use by carrying out a customized action using scripts.
Requirement 3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	Examine the permissions associated with key files and ensure that access is restricted to the fewest number of custodians necessary.	**NTFS and share permissions reporting** Receive detailed reports on the NTFS and share permissions of files and folders to know which user has what permission to them.
Requirement 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. **7.1.1** Define access needs for each role **7.1.2** Restrict access to privileged user IDs **7.1.3** Assign access based on individual personnel's job classification and 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 that individual's job function • Restricted to least privileges necessary to perform job responsibilities.	**NTFS permission reporting** List users who have access to files containing cardholder data along with details on what actions each user can perform on them. **Effective permission analysis** Ensure the confidentiality of cardholder data by analyzing and reporting on effective permissions. Verify that users do not have more privileges than required for their role. **Detection of overexposed files** Locate files that can be accessed by very employee and files that allow full control access to users.

Requirement 8.1.3 Immediately revoke access for any terminated users.	Ensure that users who have been terminated from your organization have been removed from file access lists.	**Analyze file ownership** Identify orphaned files and files owned by stale, disabled, or inactive users to prevent malicious file change attempts by terminated employees.
Requirement 10.1 Implement audit trails to link all access to system components to each individual user.	Generate audit logs that provide the ability to trace suspicious activity back to a specific user.	**Detailed audit trail** Track critical file accesses, web app usage, USB usage, printer usage, and more with a centralized access audit log. **Root cause analysis** Leverage granular report filtering options to expedite root cause analysis and identify the extent of a breach
Requirement 10.2 Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual user accesses to cardholder data **10.2.2** All actions taken by any individual with root or administrative privileges	• Audit user activity in your CDE in real time. • Track changes made by users with administrative privileges.	**File activity monitoring** Track all file and folder events—read, create, modify, overwrite, move, rename, delete, and permission change events —happening in your PCI and cardholder data storage environment. **Privileged user monitoring** List users with privileged access to sensitive files and customize reports to monitor all file changes made by them.
Requirement 10.3 Record at least the following audit trail entries for each event: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6.** Identity or name of affected data	Collect detailed logs on user activity in your CDE.	**Real-time change auditing** Get complete information on every file access, including details on who attempted what change, in which file, when, from where, and whether they were successful.

Requirement 10.5 Secure audit trails so they cannot be altered. **10.5.5** Use file integrity monitoring 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 file integrity monitoring or change detection systems to check for changes to critical files, and send notifications when such changes are noted.	**PCI file integrity monitoring** Audit every successful and failed file access attempts 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 response** Execute automated responses to minimize potential damage in the event of a security incident.
Requirement 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	Regular log reviews can identify and proactively address unauthorized access to the cardholder data environment. It also reduces the time taken 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 10.7 Retain audit trail history for at least one year with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from a backup).	It often takes a while to notice a compromise, which is why retaining logs for at least a year ensures that investigators have sufficient log history to determine the length of time 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 upload them at a later date to analyze file accesses.
Requirement 11.5 Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the tool to perform critical file comparisons at least weekly.	• 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.

11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.		**Execute custom incident responses** Automate batch files to shut down machines, end user sessions, and more.
Requirement 12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storing of cardholder data on local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	Prohibit users from storing or copying cardholder data on their local personal computers or other media unless they have been explicitly authorized to do so.	**File copy protection** Monitor file copy actions in real time and prevent the unwarranted transfer of critical data across local and network shares. **USB write-protection** Blocklist suspicious USB devices and prevent users from exfiltrating sensitive data.
Requirement A3.2.5 Implement a data discovery methodology to confirm the scope of PCI DSS and to locate all sources and locations of clear-text PAN at least quarterly and upon significant changes to the cardholder environment or processes. **A3.2.5.1** Data discovery methods must be able to discover clear-text PAN on all types of system components and file formats in use. **A3.2.5.2** Implement response procedures to be initiated upon the detection of clear-text PAN outside of the CDE to include: • Procedures for determining what to do if clear-text PAN is discovered outside of the CDE, including its retrieval, secure deletion and/or migration into the currently defined CDE	• Periodically report on the locations of cardholder data in file storage environment. • Identify sensitive data residing outside the defined CDE. • Perform remedial actions when sensitive data is discovered outside the CDE.	**Schedule-based PCI data discovery** Identify and document PCI data (including clear-text PAN) across enterprise storage. **Multi-platform visibility** Detect sensitive cardholder and PCI data across Windows file servers, failover clusters, and MSSQL databases. **Automate remediation** When sensitive files are found outside the CDE, DataSecurity Plus can be configured to automatically delete, move, or otherwise manage them. **Ownership and access analysis** Know who owns the sensitive file and trace all user actions in the time frame under analysis. This will help you determine how it ended up outside the CDE.

• Procedures for determining how the data ended up outside of the CDE • Procedures for identifying the source of the data		
Requirement A3.2.6 Implement mechanisms for detecting and preventing clear-text PAN from leaving the CDE via an unauthorized channel, method, or process, including generation of audit logs and alerts. **A3.2.6.1** Implement response procedures to be initiated upon the detection of attempts to remove clear-text PAN from the CDE via an unauthorized channel, method, or process.	Implement data loss prevention (DLP) solutions to detect and prevent leaks via emails, removable media, and printers.	**Unified data loss prevention platform** Classify sensitive data and prevent its leakage via external storage devices, Outlook, and printers. **Control peripheral device usage** Restrict the use of USB devices, wireless access points, and CD/DVD drives using central device control policies to protect against data exfiltration. **Prevent data leaks via USBs** Block USB devices in response to anomalous data transfers and attempts to exfiltrate sensitive data.
Requirement A3.4.1 Review user accounts and access privileges to in-scope system components at least every six months to ensure user accounts and access remain appropriate based on job function. **PCI DSS reference: Requirement 7**	Review users' access privileges at least every six months and verify that they are appropriate for their job functions.	**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 more to help ensure that the principle of least privilege is followed. These reports can be mailed on a set schedule to multiple stakeholders.
Requirement A3.5.1 Implement a methodology for the timely identification of attack patterns and undesirable behavior across systems—for example, using coordinated manual reviews and/or centrally managed or automated log-correlation tools—to include at least the following:	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 accesses after business hours, an excessive number of failed access attempts, and more. **Rapid alerts** Configure alerts for unwarranted changes in critical files, discovery of sensitive data outside the CDE, and more.

- Identification of anomalies or suspicious activity as it occurs - Issuance of timely 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**		**Threat detection and response** Detect ransomware intrusions and execute scripts to quarantine infected machines and prevent the spread of malware.

Disclaimer: Fully complying with PCI DSS requires a variety of solutions, processes, people, and technologies. This page is provided for informational purposes only and should not be considered as legal advice for PCI DSS compliance. ManageEngine makes no warranties, express, implied, or statutory, about the information in this material.

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