SOLUTION GUIDE

How StrongDM Helps with PCI DSS 4.0 Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a framework created by The Payment Card Industry Security Standards Council (PCI SSC). It outlines a set of policies and procedures required to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

Below are the specific requirements where StrongDM can help you achieve PCI DSS compliance.

Requirement	Description	StrongDM Feature
Requirement 1: Install and Maintain Network Security Controls		
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 at Requirement 6.5.1.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.
1.4	**Network security controls (NSCs) are configured and maintained.**	
1.4.1	NSCs are implemented between trusted and untrusted networks.	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.

Requirement	Description	StrongDM Feature
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 (including the Internet) and the CDE as follows. • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams).
Requirement 3: Protect Stored Account Data		
3.5	**PAN is secured wherever it is stored.**	
3.5.1.3	If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	StrongDM stores credentials in a hardened AWS vault. We also support customer-owned-and-maintained secret stores that can be configured for access.
3.6	**Cryptographic keys used to protect stored account data are secured.**	
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	Credentials are never exposed to the end user. StrongDM stores credentials in a hardened AWS vault. We also support customer-owned-and-maintained secret stores that can be configured for access. Access to the secret store is limited by administrator privileges.

Requirement	Description	StrongDM Feature
Requirement 6: Develop and Maintain Secure Systems and Software		
6.2	**Bespoke and custom software is developed securely.**	
6.2.1	Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
6.2.4	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities for bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.

Requirement	Description	StrongDM Feature
6.5.3	Pre-production environments are separated from production environments and the separation is enforced with access controls.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
6.5.6	Test data and test accounts are removed from system components before the system goes into production.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know		
7.2	**Access to system components and data is appropriately defined and assigned.**	
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.

Requirement	Description	StrongDM Feature
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
7.2.3	Required privileges are approved by authorized personnel.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
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. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
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. • Access is limited to the systems, applications, or processes that specifically require their use.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/ system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.

Requirement	Description	StrongDM Feature
7.3	**Logical access to system components and data is managed via an access control system(s).**	
7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
7.3.2	The access control system(s) is configured to enforce privileges assigned to individuals, applications, and systems based on job classification and function.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
7.3.3	The access control system(s) is set to "deny all" by default.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
Requirement 8: Identify Users and Authenticate Access to System Components		
8.1	**Processes and mechanisms to perform activities in Requirement 8 are defined and understood.**	
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. *New requirement - effective immediately*	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.

Requirement	Description	StrongDM Feature
8.2	**User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.**	
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
8.2.3	**Additional requirement for service providers only:** Service providers with remote access to customer premises use unique authentication factors for each customer premises.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
8.2.5	Access for terminated users is immediately revoked	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.

Requirement	Description	StrongDM Feature
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
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.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	The StrongDM Desktop App will lock due to a configured time of inactivity. Users must reauthenticate in order to access resources.
8.3	**Strong authentication for users and administrators is established and managed.**	
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.
8.3.3	User identity is verified before modifying any authentication factor.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.3.7	Individuals are not allowed to submit a new password/ passphrase that is the same as any of the last four passwords/ passphrases used.	Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.

Requirement	Description	StrongDM Feature
8.3.11	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.4	**Multi-factor authentication (MFA) systems are configured to prevent misuse.**	
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.4.3	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
8.5	**Multi-factor authentication is implemented to secure access to the CDE.**	
8.5.1	MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.

Requirement	Description	StrongDM Feature
8.6	**Use of application and system accounts and associated authentication factors are strictly managed.**	
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
8.6.2	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. Note: stored passwords/ passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.	Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	Leverage StrongDM's Access Workflows to implement just in time access to all infrastructure to eliminate standing access and reach zero standing privileges.
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data		
10.2	**Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.**	
10.2.1.1	Audit logs capture all individual user access to cardholder data.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.

Requirement	Description	StrongDM Feature
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.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
10.2.1.3	Audit logs capture all access to audit logs.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
10.2.1.4	Audit logs capture all invalid logical access attempts.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
10.2.1.6	Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
10.2.2	Audit logs record the following 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 (for example, name and protocol).	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.

Requirement	Description	StrongDM Feature
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.	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
10.3.2	Audit log files are protected to prevent modifications by individuals.	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
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.	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
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.	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
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.	All logs can be stored for 13 months or streamed to an S3 bucket or SIEM/SOAR solution.
10.7	**Failures of critical security control systems are detected, reported, and responded to promptly.**	
10.7.1	**Additional requirement for service providers only:** 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)	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.

Requirement	Description	StrongDM Feature
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).	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers		
A1.1	**Multi-tenant service providers protect and segregate all customer environments and data.**	
A1.1.1	Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.
A1.1.2	Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.	The StrongDM Admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.