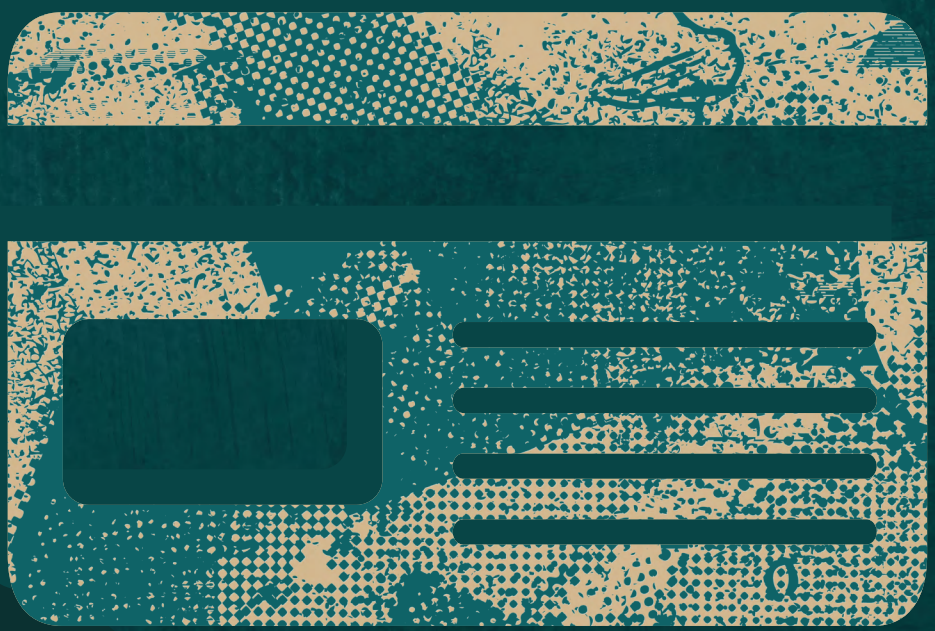
SILVERFORT

PCI DSS v4.0 Compliance with Silverfort Identity Protection

WHITE PAPER



Executive Summary

Identity protection requirements outlined in PCI DSS v4.0

On March 31, 2024, PCI Data Security Standard (PCI DSS) version 3.2.1 will be retired and replaced by PCI DSS version 4.0, following a two-year transition period.

New requirements have been added to PCI DSS v4.0, while existing requirements have been updated to keep pace with the constantly changing security demands of the payment industry. These include **enhanced multi-factor authentication (MFA) requirements, updated password requirements,** and new requirements related to secure e-commerce and anti-phishing.

Moreover, PCI DSS v4.0 requires organizations to **clearly define roles and responsibilities for setting up and managing service accounts,** group accounts, and shared accounts.

Another key element of PCI DSS v4.0 is a new concept called **targeted risk analysis (TRA).** TRAs specify **which requirements apply to each asset (log files, credentials, etc.), the outcomes from which the requirement protects the assets (malware, misuse of credentials, etc.),** and how often risk analysis is required.

Silverfort for PCI DSS v4.0

Silverfort integrates with all Identity and Access Management (IAM) products and infrastructures to achieve full visibility into all authentications and access attempts of user and service accounts. Silverfort provides ongoing risk analysis, advanced MFA and ITDR (Identity Threat Detection and Response):

Secure Networks and Systems
All network traffic is controlled by custom access policies.

Strong Access Controls
MFA is enforced on all users and all access attempts to all resources.

Continuous Monitoring
All access requests are monitored at all times in order to detect anomalies and prevent malicious access in real time.

Mapping Silverfort capabilities to PCI DSS v4.0

PCI DSS v4.0 Requirement	Silverfort Security Control
Build and maintain a secure network and systems	
1.1 Processes and mechanisms for installing and maintaining security controls are defined and understood.	Silverfort enables admins to configure and manage identity security access policies.
1.3 Network access to and from the cardholder data environment is restricted.	Silverfort's access policies can enforce a least-privileged access approach, ensuring access to critical resources in the environment is restricted and monitored.
1.4 Network connections between trusted and untrusted networks are controlled.	Silverfort's access policies can be configured based on source and destination networks to enforce MFA or block access on user accounts that connect from one network to another.
Implement strong access control measures	
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	Silverfort's access policies are configured based on the users, groups, and OU from the directories in the environments. As such they can be applied to users based on their privileges and organizational classifications, allowing admins to create access groups and monitor log files to detect malicious or irregular activity.
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.	Silverfort provides full visibility into all user accounts' authentication trails, while alerting on any excessive access requests and detected malicious activity. This allows admins to perform scheduled, continuous and as-needed security reviews.

PCI DSS v4.0 Requirement	Silverfort Security Control
Implement strong access control measures	
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. **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.	Silverfort provides fully automated visibility and monitoring of system/service accounts. This includes classification of pure machine-to-machine accounts, accounts that are used interactively, and accounts that access a significant number of destinations. Additionally, each account's sources, destinations, privilege level, and risk score are aggregated and displayed. This enables admins to regularly monitor accounts' activities and immediately flag any excessive access. To address inappropriate access and potential compromise, Silverfort also auto-creates an access policy to each system/service account that, when enabled, blocks any access attempt that deviates from the service account's normal behavior. As a result, even if an adversary attempts to use a compromised service account for malicious access, they will get blocked.
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	Silverfort provides admins with a detailed log screen that documents every authentication and access attempt carried out in the environment. The log screen includes optional filters to detect insecure authentications, suspicious activity, misconfiguration and other anomalies.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Silverfort enables admins to monitor and configure access policies to users across their entire lifecycle. Additionally, Silverfort detects any stale accounts, unchanged passwords and other indications that an existing user account is no longer active.
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	Silverfort detects all inactive user accounts, enabling admins to easily identify and remove them.
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.	Silverfort enables admins to monitor all third-party authentication requests, as well as detect and prevent their abused by adversaries for malicious access.

PCI DSS v4.0 Requirement	Silverfort Security Control
Implement strong access control measures	
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.	Silverfort allows admins to enforce MFA on any activity or under any circumstance they deem appropriate, such as when a user is idle for a specified period.
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. **8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access. **8.4.2** MFA is implemented for all access into the CDE. **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. **8.5** Multi-factor authentication (MFA) systems are configured to prevent misuse. **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.	Silverfort can enforce MFA on any access request, whether on-prem, remote, or third-party, and for every level of credentials, from regular users to admins. In an Active Directory (AD) environment, Silverfort can enforce MFA and block access policies on any LDAP\S, NTLM, and Kerberos authentications. This expands the scope of MFA protection to a wide array of resources and access methods that couldn't have been protected before, such as command line tools, legacy applications, IT infrastructure and more. Silverfort ensures no access is granted based on passwords alone, and users are required to authenticate through MFA to verify that they are who they claim to be.

PCI DSS v4.0 Requirement	Silverfort Security Control
Implement strong access control measures	
8.6 Use of application and system accounts and associated authentication factors is 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 the account is granted. • Every action taken is attributable to an individual user.	Silverfort provides fully automated visibility and monitoring of system/service accounts. This includes classification of pure machine-to-machine accounts, accounts that are used interactively, and accounts that that access a significantly large number of destinations. Additionally, each account's sources, destinations, privilege level, and risk score are aggregated and displayed. This data enables admin to determine whether the interactive use of these types of accounts is justified or should be banned and apply the steps described in 8.6.1 section.
Regularly monitor and test networks	
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.	Silverfort provides admins with a detailed log screen that documents every authentication and access attempt carried out in the environment. The log screen includes optional filters to detect insecure authentications, suspicious activity, misconfiguration and other anomalies.
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.	Silverfort logs capture the activities of all users, including accounts with administrative access privileges and system/service accounts.
10.2.1.3 Audit logs capture all access to audit logs. **10.2.1.4** Audit logs capture all invalid logical access attempts.	Silverfort detects and alerts of any invalid access attempts that were invalidated due to wrong passwords or MFA/access block policies.

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

For more information, visit silverfort.com