Symantec
by Broadcom

WHITE PAPER

Addressing PCI Compliance

The Critical Role of Privileged Access Management

WHITE PAPER

Addressing PCI Compliance

The Critical Role of Privileged Access Management

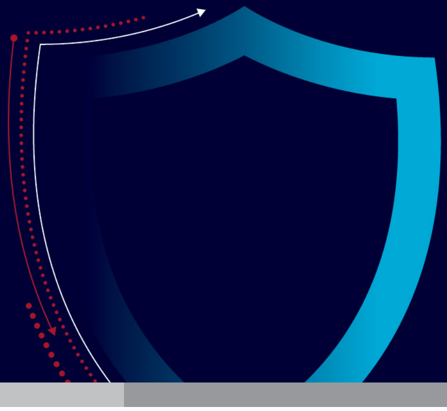

TABLE OF CONTENTS

Introduction

In today's digital landscape, protecting sensitive payment card data is more critical than ever. The Payment Card Industry Data Security Standard (PCI DSS), established in 2004, enhances security controls to protect cardholder data from breaches and fraud. Businesses that process, store, or transmit payment information must comply with PCI DSS's stringent security requirements. However, validation remains a significant challenge. According to the 2024 Verizon Payment Report, only 14% of organizations were entirely PCI DSS compliant in 2023 under version 3.2.1. Most businesses have yet to be audited against the newer 4.0.x revision.

PCI DSS has evolved to keep pace with the ever-changing cybersecurity landscape and emerging threats. Early versions focused on fundamental security measures such as firewalls, encryption, and access controls. However, as cyber threats became more sophisticated, updates introduced more substantial authentication requirements, enhanced encryption standards, and stricter controls for third-party service providers. The release of PCI DSS 4.0 in 2022 marked a significant shift, emphasizing continuous security monitoring, a risk-based approach, and greater flexibility in how organizations achieve compliance.

A Critical Factor in PCI DSS Compliance: Managing Privileged Access

Managing privileged access across an organization's systems is one of the most challenging aspects of achieving PCI DSS compliance. Cybercriminals frequently target privileged accounts because they access an organization's most sensitive data and infrastructure. Without proper controls, these accounts become the weakest link in an otherwise secure environment.

Before PCI DSS 4.0, implementing a privileged access management (PAM) solution was optional, but it is now essential. Privileged identities are often overlooked—until a breach or compliance failure exposes the risks. These accounts exist throughout an organization, from IT administrators to application-to-application (A2A) interactions, and their scope is expanding with digital transformation. Privileged accounts remain prime cyberattack targets, given their broad access and potential for misuse.

Organizations must enforce strict security measures for privileged access to mitigate these risks. These measures strengthen security posture and ensure compliance with regulatory mandates like PCI DSS 4.0.

Where Symantec PAM Helps Protect Cardholder Data

Attackers follow an established pattern: gaining access, elevating privileges, moving laterally, and escalating until they reach their ultimate target. Symantec PAM is designed to protect administrative credentials and other secrets, while controlling privileged access across cloud, physical, and virtual environments. The solution delivers five core services: privileged credential vault, session management and recording, behavioral analytics, fine-grained access controls, and secrets management from a single platform. Additionally, Symantec PAM provides several key capabilities to disrupt the attack cycle:

SYMANTEC PAM IS DESIGNED TO PROTECT ADMINISTRATIVE CREDENTIALS AND OTHER SECRETS

- Multifactor Authentication (MFA): Strengthens security by requiring multiple credentials to access privileged accounts.
- Least Privilege Enforcement: This policy restricts what privileged accounts can execute commands within the cardholder data environment (CDE), limiting unauthorized data access.
- Network Segmentation: Controls which subnets privileged accounts can access, preventing lateral movement and reducing attack visibility.
- Socket Filter Agent (SFA): Blocks unauthorized network connections, ensuring administrators can only access systems permitted by Symantec PAM policies.

By integrating these controls, Symantec PAM helps organizations safeguard their most critical assets, maintain compliance with PCI DSS 4.0, and reduce the risk of breaches caused by compromised privileged accounts.

Addressing PCI DSS 4.0.1 with Symantec PAM

This section describes how Symantec PAM addresses the PCI DSS 4.0.1 requirements.

Requirement 8: Identify Users & Authenticate Access

Symantec PAM ensures secure, controlled, and monitored privileged access by enforcing strong authentication policies, managing privileged accounts, identifying user actions, and preventing unauthorized access. As Symantec PAM delivers these capabilities, nearly all of section 8 can be covered by adequately implementing them. The key requirements covered by PAM are shown in the following table.

SYMANTEC PAM COVERS NEARLY ALL OF DSS REQUIREMENT 8

Requirement	How PAM Addresses
8.2.1 - All users are assigned a unique ID before access to system components or cardholder data is allowed.	While this may be interpreted as a prohibition on shared accounts, the main goal is the ability to trace actions back to an individual. Even if shared accounts are used to access endpoint systems with PAM, the usage of that account can be traced back to the individual. As long as the user accesses PAM with a unique ID, all further actions are recorded under that individual's ID.
8.2.2 - Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary, on an exception basis.	Most systems are delivered with built-in accounts. The first step is to vault these accounts in PAM so that any time they are used, actions can be attributed back to an individual user.
8.2.4 - Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed.	With PAM protecting any systems that would allow the modification of user IDs, this access can be set only to allow specific permissions and a workflow added for necessary approvals.
8.2.5 - Access for terminated users is immediately revoked.	The immediate revocation of access has historically been challenging when many systems and teams are involved. However, with all PCI scoped system access through PAM, simply disabling the user account that would access PAM inherently disables all downstream access. This is the case irrespective of the authentication type such as Local, SAML, Active Directory, or smart card.
8.2.6 - Inactive user accounts are removed or disabled within 90 days of inactivity.	Building on 8.2.5, inactive PAM user accounts may be set for disablement after a set period of inactivity.
8.2.7 - Accounts used by third parties to access, support, or maintain system components via remote access are managed.	Third-party access should only be enabled during the time period needed, and use should be monitored for unexpected activity. PAM allows for time-based access as well as approval workflows that disable access until approved. With PAM Threat Analytics, user behavior is monitored using machine learning that detects any anomalies with system access, such as logging in during an abnormal time or from a new/disallowed location.
8.2.8 - Disconnect user idle sessions.	PAM may be set to disconnect user sessions after a set period of inactivity and require re-authentication.
8.3.x - Strong authentication for users and administrators is established and managed.	Many of the 8.3 requirements are covered by the PAM solution: • Multi-factor authentication • Strong cryptography during authentication • Invalid authentication attempts are limited • Passwords are forced to be reset immediately after first use • Passwords require a minimum length of 12 characters • Passwords are not allowed to be re-used (last 4) • Passwords are changed at least every 90 days
8.4.x - MFA is implemented for all non-console access to the CDE.	PAM enforces MFA for privileged users, ensuring only authorized personnel can access sensitive systems. Many systems, especially legacy systems, may present a challenge when implementing MFA at a large scale. Service accounts that do not have MFA capability may also be used. However, if systems are only accessible through PAM, MFA is enforced to these downstream systems.
8.6.1 - Use of service accounts is strictly managed.	Should a service account require interactive login, controlling access through PAM provides the necessary requirements for the section, including approvals, time limits, individual attribution, and business justification.
8.6.2 - Passwords/passphrases are not hard coded in scripts.	Levering the PAM Application to Application (A2A) solution, scripts may provide the necessary credentials at runtime instead of hardcoding the credentials. Additional security options when using A2A include verification of the script hash, file location, and account used to execute the script.
8.6.3 - Passwords/passphrases for system accounts are changed periodically with sufficient complexity.	Password composition policies in PAM allow for specific complexity requirements and password age, with automatic credential updates before the specified age.

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

PAM provides full session recording, auditing, and real-time alerting to detect unauthorized activities. Exporting logs to a central SIEM is supported, and any activity logs stored in PAM are protected from unauthorized change or deletion.

Requirement	How PAM Addresses
10.2.1 - Audit logs are enabled and active for all system components and cardholder data	Any system access through PAM will be recorded for playback, along with details about the connection (end user, end user location/address, time, etc.). In addition, the Threat Analytics for PAM solution uses behavior analytics to automatically mitigate suspicious behavior and provide reports for any audit or incident.
10.3.1 - Read access to audit logs is limited to those with a job-related need.	Role-based access within PAM permits only authorized users to review logs and recordings.
10.3.2 - Audit logs are protected to prevent modifications by individuals	All logs stored in PAM are protected from deletion and modification.
10.3.3 - Audit log files are promptly backed up to a central log server	All PAM logs may be forwarded to a central SIEM via Syslog.

Requirement 6: Develop and Maintain Secure Systems and Software

Development and automation activities in a PCI environment require the same level of protection using PAM. In this section, PAM may cover securing custom software development and changes to system components.

Requirement	How PAM Addresses
6.4.3 - Organizations must ensure that all scripts executed in payment environments are authorized and documented	PAM Application to Application (A2A) solution performs script integrity validation before allowing/providing authentication to the defined systems. The script inventory may be reviewed within the PAM console.

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

As a central gateway to a cardholder data environment, PAM provides many benefits for controlling and auditing any PCI-scoped access.

AS A CENTRAL GATEWAY TO A CARDHOLDER DATA ENVIRONMENT, PAM PROVIDES MANY BENEFITS FOR CONTROLLING AND AUDITING ANY PCI-SCOPED ACCESS

Requirement	how PAM Addresses
7.2.6 - All user access to cardholder data is restricted based upon user roles	With PAM controlling the credentials to the CDE and end users not knowing the credentials, access is limited to only the allowed methods within PAM. PAM's role-based access control, combined with time-based access and dual authorization, ensures that direct access is documented and approved.
7.3.1 - Access to system components and data is managed via an access control system	A core functionality of PAM, any access is restricted outside of the defined/permitted access within PAM.
7.3.3 - The access control system is set to "deny all" by default	End users in PAM are not granted access to any system or action, and it is built upon a "deny all" by default model.

Requirement 2: Apply Secure Configurations to All System Components

Historically, enterprises face several primary challenges with default accounts. The first is that default accounts are often administrative and are required to perform key activities, so removing or blocking access to them is not a feasible option. The second is that these accounts generally provide unrestricted access and permissions. And finally, default accounts are often shared by multiple internal and sometimes external individuals. Symantec PAM enhances security by protecting privileged credentials and controlling privileged access across all IT resources.

Requirement	How PAM Addresses
2.2.2 - Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	Symantec PAM manages the lifecycle of credentials. Bringing vendor accounts under management in PAM allows application of complex secure Password Composition Policies, unique SSH keys or protected access to other secrets used to access vendor default accounts. The solution can also automatically rotate these credentials to comply with internal policies and security mandates.

Defining the Scope of PCI Compliance

PAM CAN HELP REDUCE THE NUMBER OF SYSTEMS IN-SCOPE FOR A PCI AUDIT

Another critical aspect of achieving PCI compliance is properly scoping systems for the audit, and PAM can help reduce the number of in-scope systems. With PAM as a gateway to the CDE, this can prevent many systems, such as end user workstations, from becoming in-scope for a PCI audit. One way you can look at PCI scoping is by using an A, B, C system:

- A class (in-scope): System stores, processes, or transmits credit card data
- B class (in-scope): System directly communicates with an A system
- C class (out of scope): System communicates with a B system - cannot communicate with an A system.

PAM may be scoped as B-class for managing credentials and brokering connections to A-class systems. This would then allow workstations and other servers leveraging PAM for CDE access to be classified as a C (out-of-scope) system. Segmentation would still be required, and the C-class system should have no network connectivity outside the defined PAM access.

Final Thoughts

Achieving and maintaining PCI DSS compliance is a complex yet essential task for organizations handling payment card data. Symantec PAM is critical in securing sensitive systems, mitigating the risk of unauthorized access, and ensuring compliance with PCI DSS requirements. By implementing strong access controls, continuous monitoring, and least privilege principles, businesses can streamline PCI audits and enhance their overall security posture. As cyber threats evolve, a proactive approach to privileged access is key to avoiding compliance challenges while protecting payment information.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

PAM-addPCIcom-WP100 April 25, 2025