Teleport

Address Key PCI DSS 4.0 Compliance Requirements With Teleport

Contents

Introduction

Financial services organizations remain a prime target for cyberattacks; they are 2.5 times more likely to experience a data breach than organizations in other industries (Verizon, Data Breach Investigations Report 2023). Yet at the same time, financial services are under enormous pressure to introduce cutting-edge capabilities to stay competitive. This requires the deployment of more and more infrastructure within already complex, highly diverse IT environments — ultimately increasing their risk exposure and infrastructure management burden.

Operational agility and innovation are critical to business performance and growth, and the pressure to efficiently scale infrastructure has never been greater. Balancing this expansion and prioritizing agility alongside security and compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) version 4.0, can feel like a tightrope walk — and it is. For many engineering teams, the drive for agility directly clashes with the need to enforce robust security and compliance protocols, ultimately creating friction that slows down development and day-to-day operations.

This friction becomes most apparent in the area of access controls, where modern, distributed, and ephemeral infrastructure collides with the strict requirements set by PCI DSS 4.0 — which goes into effect on March 31, 2025. Financial services organizations and other companies dependent upon cardholder and payment data processing need a way to improve developer productivity without compromising security or risking PCI non-compliance during an audit.

PCI DSS is one of the oldest mainstream requirements for compliance, originating in 2004. The PCI Security Standards Council manages the standard to ensure security for the global payment system. It applies to all entities that store, process, or transmit payment cardholder data or sensitive authentication data or could impact the security of the cardholder data environment (CDE). There are ten PCI DSS 4.0 controls outlined in this paper — grouped by **Access Management**, **Audit Logging**, **Data Protection**, and **Change Control** — that become problematic for financial services organizations as they scale their use of modern infrastructure.

Teleport, a secure infrastructure access platform, removes the root causes of tension between engineering, compliance and security teams. This white paper highlights common PCI DSS control hurdles organizations face as they scale modern infrastructures, and provides practical solutions for implementing these controls in a way that strikes the delicate balance of agility, security, and compliance.

Two-thirds of engineering and security professionals reported slowing down or delaying application development due to Kubernetes security concerns. (Red Hat)

Access Management

PCI DSS 4.0 mandates strict isolation of sensitive data environments, but as teams grow and infrastructure becomes more complex and heterogeneous, maintaining this separation — while still enabling developers to do their jobs — becomes a monumental challenge. The root of the problem lies in the inefficiency of traditional credential-based access systems, which simply do not scale to meet the demands of modern infrastructures.

This section explores several selected examples of where this approach breaks down and can cause inefficiencies when aligning to the framework of PCI DSS. Though not intended to be a comprehensive mapping of the standard, you will find an illustration of Teleport use cases for solving key PCI DSS challenges.

PCI DSS 4.0 Requirement 2.2

All system components are configured and managed securely.

The challenge

In the context of modern infrastructure, this means ensuring that sensitive and non-sensitive workloads are segregated across namespaces or clusters, rather than co-locating them in the same environment. This separation helps protect cardholder data (CHD) and other sensitive information. Also, subcategory 2.2.6 says system security parameters must be configured to prevent misuse.

How Teleport supports compliance

Teleport provides centralized access control and monitoring, ensuring only highly authorized and authenticated users can modify system configurations.

Detailed audit logging and session recording capabilities enable organizations to track and review changes to system settings, helping to prevent unauthorized alterations. Role-based access control (RBAC) enforces the principle of least privilege, limiting user access to only necessary services and significantly reducing misconfiguration risks.

PCI DSS 4.0 Requirement 6.5

Changes to all system components are managed securely.

The challenge

System components are broadly defined by PCI to include almost all infrastructure elements, including container clusters like Kubernetes.

For environments using Kubernetes, this requirement mandates enforcing strict controls over how namespaces or clusters are used for development versus production workloads. Misconfiguration or accidental deployment to the wrong namespace can violate compliance requirements and expose sensitive cardholder or payment data. Subcategory 6.5.3 requires access control enforcement for the separation of pre-production from production environments, which can create several challenges.

How Teleport supports compliance

Teleport provides fine-grained access controls to foundational system components, cloud environments, and container platforms, including Kubernetes clusters.

Intuitive RBAC capabilities enforce the principle of least privilege down to the namespace level, giving your team the ability to tune user privileges and access permissions to the levels requested by PCI, and for production versus pre-production environments, even within recently provisioned Kubernetes deployments.

PCI DSS 4.0 Requirements 7.1 and 7.2

Limit access to system components and cardholder data to only those individuals whose job requires such access. Access to system components and data is appropriately defined and assigned.

The challenge

Accurately defining and documenting who needs access to sensitive data can be extremely complex. Ensuring that access controls are consistently evaluated, enforced, and updated in response to personnel changes or business requires heavy involvement from engineering and security teams, which can slow down operations. Subcategory 7.2.1 through 7.2.5 discuss the need to properly grant access and manage access privileges.

Failure to meet these requirements exposes resources with sensitive cardholder and payment data to threats, and can pose a major challenge to organizations seeking PCI compliance.

How Teleport supports compliance

Teleport enforces strict role-based access control (RBAC) policies across critical infrastructure, including cloud environments (like Kubernetes or AWS). This ensures users and services are granted the least privilege necessary to perform their functions, preventing unauthorized access to cardholder data.

Comprehensive visibility into access activities and audit logs make it simpler for your teams to identify unauthorized access and quickly make the policy changes as necessary to remediate. Ephemeral privileges bound to biometric devices and secure enclaves are used for all access requests, removing the need for super-privileged accounts entirely.

Teleport

Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.