Framework Foundations: PCI DSS

Introduction to PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework developed by the PCI Security Standards Council (PCI SSC) to help organizations protect cardholder data and reduce credit card fraud. It is mandated by major card brands including Visa, Discover, MasterCard, American Express, and JCB.

PCI DSS applies to any organization that stores, processes, or transmits payment card data. This includes merchants, payment processors, service providers, and third-party vendors that impact the security of the cardholder data environment (CDE).

The standard is structured around four ongoing steps:

- **Assess:** Identify and evaluate systems that handle cardholder data.
- **Remediate:** Address security gaps and remove unnecessary data.
- **Report:** Document compliance efforts and submit reports to acquiring banks or card brands.
- **Monitor and Maintain:** Integrate security into daily operations and continuously monitor controls.

Objectives of PCI DSS

PCI DSS is designed to help organizations:

- Protect cardholder data from unauthorized access or theft.
- Reduce the risk of data breaches and fraud.
- Establish consistent security practices across systems and networks.
- Promote accountability through regular assessments and reporting.
- Safeguard sensitive payment data to maintain customer trust.

Key Requirements

PCI DSS is structured around 12 core requirements, grouped into six overarching goals. These requirements reflect widely accepted security practices and are designed to help organizations protect cardholder data throughout its lifecycle – from storage and transmission to access and monitoring.

Rather than viewing the requirements as a checklist, PCI DSS encourages organizations to adopt a continuous security mindset. This includes:

- Building secure systems and networks that limit exposure to threats.
- Protecting cardholder data through encryption and access controls.
- Managing vulnerabilities with timely updates and malware defenses.
- Controlling access to sensitive systems and data based on business need.
- Monitoring and testing systems regularly to detect and respond to anomalies.
- Embedding security policies into daily operations and organizational culture.

These requirements apply to all entities that store, process, or transmit cardholder data, including merchants, service providers, and third-party vendors. The PCI Security Standards Council also emphasizes the importance of integrating these controls into “business-as-usual” processes to maintain security year-round.

How Cisco + Splunk Support Compliance

PCI DSS Goal	PCI DSS Core Requirement	How Cisco + Splunk Support Compliance	Relevant Products
Build and Maintain a Secure Network and Systems	Install and maintain network security controls	Segments and monitors networks to prevent unauthorized access	Cisco Secure Firewall, Cisco Umbrella, Ciso Identity Services Engine (ISE), Cisco Secure Network Analytics (SNA), Cisco SD-WAN, Cisco Hypershield, Splunk enterprise Security (ES), Splunk App for PCI Compliance
	Apply secure configurations to all system components	Configures systems securely to reduce vulnerabilities	Cisco Secure Firewall, Cisco Secure Endpoint, Cisco ISE, Cisco Catalyst Center, Splunk ES
Protect Account Data	Protect stored account data	Secures sensitive data from unauthorized access	Cisco Secure Endpoint, Cisco Umbrella, Cisco Secure Firewall, Splunk ES
	Protect cardholder data with strong cryptography during transmission over open, public networks	Encrypts data during transmission to prevent interception	Cisco Secure Firewall, Cisco Duo, Cisco SD-WAN, Splunk ES
Maintain a Vulnerability Management Program	Protect all systems and networks from malicious software	Detect and block malware across systems	Cisco Secure Endpoint, Cisco Umbrella, Cisco Talos Intelligence, Cisco SNA, Splunk ES, Splunk SOAR
	Develop and maintain secure systems and software	Manages secure development and ongoing system security	Cisco XDR, Cisco Secure Firewall, Splunk ES, Splunk SOAR

PCI DSS Goal	PCI DSS Core Requirement	How Cisco + Splunk Support Compliance	Relevant Products
Implement Strong Access Control Measures	Restrict access to system components and cardholder data by business need-to-know	Limits access to system components and cardholder data to authorized users only	Cisco ISE, Cisco Duo, Cisco Secure Firewall, Splunk ES
	Identify users and authenticate access to system components	Verifies user identity before granting access	Cisco Duo, Cisco ISE, Cisco Secure Firewall, Splunk ES
	Restrict physical access to cardholder data	Secures physical access to sensitive systems	Cisco Meraki MV (video surveillance), Splunk ES
Regularly Monitor and Test Networks	Log and monitor all access to system components and cardholder data	Tracks and monitors access for suspicious activity	Cisco SNA, Cisco XDR, Splunk ES, Splunk App for PCI Compliance, Splunk Cloud Platform
	Test security of systems and networks regularly	Conduct regular security assessments	Cisco Secure Firewall, Cisco Catalyst Center, Splunk ES, Splunk SOAR
Maintain an Information Security Policy	Support information security with organizational policies and programs	Manages and enforces security policies across the organization	Cisco XDR, Cisco Secure Firewall, Splunk ES, Splunk SOAR

PCI DSS Compliance with Cisco Security + Splunk

Meeting the requirements of PCI DSS is a necessary step for organizations that handle payment card data. The framework provides a structured approach to managing risk, protecting sensitive information, and maintaining accountability across systems and processes.

Cisco and Splunk offer a range of technologies that support these efforts. Our tools help organizations implement access controls, monitor activity, detect threats, and manage vulnerabilities in ways that align with PCI DSS expectations. By mapping products to each of the 12 core requirements, organizations can better understand how to apply technical solutions to meet security and reporting needs.

As threats evolve and compliance standards continue to adapt, having a clear view of how existing tools contribute to PCI DSS goals can help teams make informed decisions and maintain a consistent approach to protecting cardholder data.

Resources

For more information and guidance on PCI DSS compliance, please refer to the following resources:

- PCI Compliance with Meraki
- PCI DSS v4.0 At-a-Glance
- PCI DSS v4.x Quick Reference Guide