Talos MSSP – Products and Services for implementing Payment Card Industry Data Security Standard

Compliance with PCI DSS

This white paper presents information about the Payment Card Industry (PCI) Data Security Standard (DSS) and how Talos MSSP assists in fulfilment of requirements in its implementation. PCI DSS is applicable to any entity that accepts credit cards as a payment method or that stores, processes, or transmits a cardholder's data.

PCI DSS overview

PCI-DSS is an information security standard for organizations that handle credit cards from the major credit card schemes. Created by the major credit card providers to reduce fraud, the standard aims to ensure that merchants storing, transmitting or processing card data meet specific security standards. It was released in 2004 and has since undergone three major revisions. The latest version of this standard was released in May 2018 (as of January 2019).

The standard is administered by an organization called Payment Card Industry Security Standards Council (PCI-SSC), which consists of the five major credit card brands: American Express, Discover, JCB International, MasterCard, and Visa Inc.

What is PCI DSS?

- PCI DSS standard is structured across six main control objectives, each with sub-requirements. These six control objectives are further divided into 12 high-level requirements (Table 1).
- PCI DSS applies to all entities that engage in card processing, including merchants, processors, acquirers, issuers, and all other payment service providers.
- PCI DSS also applies to all entities that store, process, or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD).

Note: This white paper does not discuss the entire set of PCI DSS requirements. It focuses mainly on services which Talos MSSP makes available for client to achieve requirements of the standard.

Contents

Table 1. PCI DSS goals and requirements

Goals	Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Protect all systems against malware and regularly update antivirus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for employees and contractors

Compliance

In general, any merchant or service provider that stores, processes or transmits cardholder data is required to comply with PCI-DSS. Compliance is a large undertaking; the main security goals may already be covered within a wider security programme, but the overall requirements can be as lengthy as 288 specific controls or requirements. Organizations have varying levels of controls depending on the type of organization and the number of transactions processed per year. Organizations are divided into four categories as shown below Table 2. The categories are complex and differ based upon card brands and geographic regions.

Table 2. Categories

Category	Criteria
Level 1	Merchants that process more than 6 million transactions per year. All wallets, processors and service providers.
Level 2	Merchants that process between 1 and 6 million transactions per year All data storage and payment facilitators with > 300,000 transactions annually.
Level 3	Merchants that process between 20,000 and 1 million transactions per year.
Level 4	All other Merchants

Level 1 entities pose the greatest risk due to the volume of card data that they are processing and, as such, have the most stringent requirements with on-site audit being conducted yearly.

Other levels usually require self-assessment and quarterly scans by an Approved Scanning Vendor (ASV); however, they may elect to certify against a higher standard.

Enforcement

The standard is enforced by the major banks, many of whom are proactive in ensuring their merchants service account holders comply. The approaches to non-compliance differ from bank to bank but have included fixed fines or surcharges per transaction. If a breach is detected and card data is lost, merchants can be fined heavy fines per compromised card.

Approved Scanning Vendors (ASV)

ASVs are companies certified by the PCI-SSC to help implement certain PCI-DSS requirements. They validate a company's compliance with the PCI-DSS and give you a certification so that you can prove compliance to your customers and acquiring bank. For a complete list of vendors, refer to the QSA approved scanning vendors on the PCI security standards website.

PCI Qualified Security Assessor

Qualified Security Assessor (QSA) is a title awarded by the PCI-SSC to individuals who have undergone PCI training and are employed by a QSA approved auditing firm; their remit is to perform PCI compliance assessments, as they relate to the protection of credit card data.

Self-assessment Questionnaire (SAQs)

There are several versions of the self-assessment questionnaire available, and the one that is needed to be completed depends upon your type of organization and how you conduct payment processing. Once the correct form has been selected, it consists of a series of yes/no questions in relation to PCI security. The way payments are processed will also determine whether the company needs ASV or pen-testing.

Talos Cybersecurity as MSSP for PCI DSS Compliance Software and Services

PCI DSS compliance software is a must-have for any organization that handles credit card data or other types of payment card data. Failure to comply can result in PCI DSS penalties and fines imposed daily, and a data breach resulting from non-compliance could cost millions in settlements, legal fees, and loss of reputation.

Yet, many IT security teams struggle to meet the many security technology requirements defined by PCI DSS 3.2. It can be difficult to know which security tools you need to achieve PCI DSS compliance. It doesn't help that organizations are often racing to get ready for their next, fast-approaching PCI audit.

Talos Cybersecurity MSSP combines the essential security technologies needed to demonstrate compliance, including asset discovery, vulnerability assessment, log management, file integrity monitoring, and others. This includes compliance reports automatic threat intelligence updates, helping to stay in compliance with continuous security monitoring.

Multiple PCI DSS Compliance Services provided

- Asset Discovery and Inventory
- Availability Monitoring
- Vulnerability Assessment
- Intrusion Detection (IDS)
- File Integrity Monitoring (FIM)
- SIEM Event Correlation
- Log Management & Monitoring
- PCI DSS Compliance Reporting

Address the Most Challenging PCI DSS Requirements

- PCI Requirement 5: Protect all systems against malware
- PCI Requirement 6: Develop and maintain secure systems and applications
- PCI Requirement 10: Track and monitor all access to network resources and cardholder data
- PCI Requirement 11: Run vulnerability scans at least quarterly, and after any significant change in your network
- PCI Requirement 12: Implement an Incident Response Plan

Summary

Many businesses do not have the tools, knowledge, and resources to fulfill the requirements for PCI Compliance. Talos Cybersecurity MSSP plays a pivotal role delivering the technologies necessary to achieve PCI compliance.

[Contact](#) Talos Cybersecurity Team or visit www.taloscybersecurity.com

Additional information

PCI DSS resources

- PCI DSS official website
- PCI DSS document library
- Qualified Security Assessors
- Approved scanning vendors
- Best practices

Software Partner

- AT&T Cybersecurity