DATA SHEET

PCI Compliance Solutions

Driven by increasing identity theft and frequent headlines about data breaches at some of the biggest organizations, the major payment card brands developed the Payment Card Industry Data Security Standard (PCI DSS) to enhance the security controls protecting payment card data from theft and misuse.

The PCI Data Security Standard

PCI DSS applies to any organization that transmits, processes or stores payment card transactions or cardholder information. The PCI standards consist of six key objectives spanning 12 major requirements.

The PCI standards require organizations to build, maintain and monitor a secure network to protect cardholder data, as well as maintain a vulnerability management and information security program. Regardless of how many transactions they process, merchants must demonstrate PCI compliance annually. Those that are not PCI compliant can face steep fines from their acquiring banks, and in some cases, have their payment card privileges revoked. As with other regulations and guidelines, PCI DSS compliance cannot be achieved through technology alone. It requires establishing and maintaining a PCI program that incorporates the appropriate policies, procedures and technology to ensure ongoing compliance through continuous protection of payment card data that is collected, stored or transmitted.

Expert Testing, Analysis and Assessments

- Highly Credentialed Experts passionate about security
- Focused on security Best Practices for your industry
- Deep understanding of Compliance, Regulations and Security Frameworks
- Latest threat intelligence from Dell SecureWorks CTU research team
- Risk based approach

Dell SecureWorks' PCI Compliance Solutions

To help businesses achieve and maintain compliance with PCI DSS and protect payment card data, Dell SecureWorks ® provides services to support organizations' PCI activities throughout all stages – from building a PCI program to performing the assessments required to demonstrate compliance.

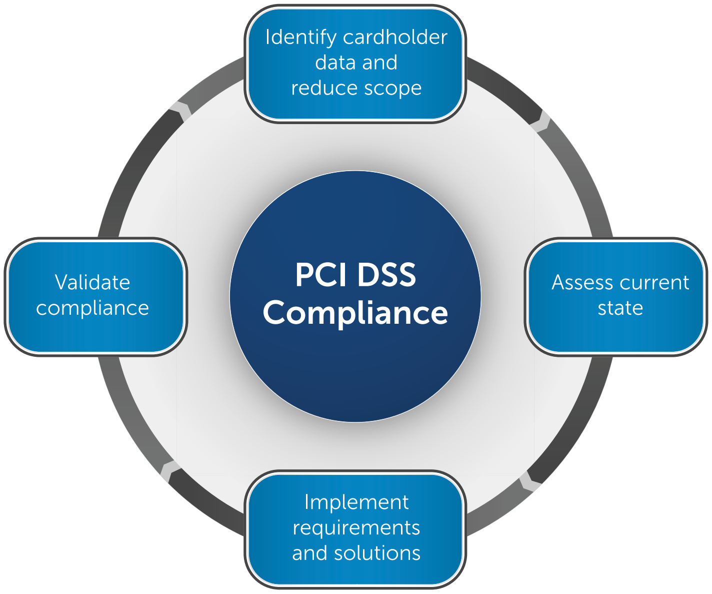
1. Identify Cardholder Data and Reduce Scope

Designed to identify how cardholder data flows, where it resides and how to design networks to properly segment the cardholder data; this phase focuses on reducing what is considered in scope for PCI DSS, in order to minimize the cardholder data footprint and reduce costs.

Dataflow Analysis

Through interviews, documentation, and network reviews, Dell SecureWorks identifies and analyzes the flow of cardholder data throughout the network. This includes identifying where all transactions occur, including data processing and storage.

Dell SecureWorks PCI Compliance Solution


Identify cardholder data and reduce scope
Assess current state
Implement requirements and solutions
Validate compliance
PCI DSS Compliance

Mapping Cardholder Data

Through interviews, documentation review, network infrastructure review and data discovery across the network, Dell SecureWorks inventories where cardholder data resides on the network. This includes identifying the systems and users that have access to the data.

PCI Data Segmenting

After determining how cardholder data flows and where it resides, Dell SecureWorks identifies and designs the best network architecture to consolidate where cardholder data is transmitted, processed and stored. This can effectively reduce how much of an organization's IT environment is truly in scope for PCI DSS, minimizing the effort and costs associated with achieving and maintaining compliance.

Merchant and Service Provider Level Classification

Based on interviews and analysis, Dell SecureWorks determines what level of compliance an organization is subject to for PCI DSS. This involves determining the merchant or service provider level.
Once classified, Dell SecureWorks identifies the requirements that must be met in order for the organization to demonstrate compliance.

Dell SecureWorks uses a four-phased approach to assist organization in their PCI compliance programs

2. Assess Current State

This phase reviews an organization's current state, identifies any areas of potential noncompliance and creates remediation plans to achieve compliance.

PCI Gap Analysis

Dell SecureWorks assesses an organization's current environment against the entire PCI DSS v3.0 standard using a combination of network architecture and documentation review, policy and procedure review and observation of system component configurations. This identifies where gaps and opportunities for improvement exist to meet DSS requirements.

Self-Assessment Questionnaire (SAQ) Assistance

Dell SecureWorks can aid organizations who need to complete the Self-Assessment Questionnaire and seek assistance from an unbiased third party with PCI expertise. The SAQ is an organization's attestation to meeting the requirements – not just a simple yes/no assessment. Organizations such as payment processors or merchant banks may request evidence of a compliant SAQ.. Ensuring the SAQ is accurate and complete is critical.

Remediation Plan Development

At the completion of the Gap Analysis or SAQ, Dell SecureWorks will develop detailed plans for remediation that are designed to meet the DSS requirements. Remediation guidance includes best practice advice and custom control creation to meet the intent of any identified gap.

Remediation assistance

Dell SecureWorks can provide assistance, consulting and advisory services in the implementation of remediation plans. This may include developing specific implementation plans or consulting on various remediation needs.

3. Implement Controls and Solutions

This phase focuses on implementing solutions that help organizations meet specific DSS requirements. In some cases, this can be in the form of consulting services to develop specific policies or procedures. In others, it might involve performing consulting services to fulfill specific requirements such as Penetration Testing and Web Application Assessments.

Dell SecureWorks also provides Information Security.

Services to meet other PCI DSS requirements, such as:

- Policy Development
- Development of System Configuration Standards
- Ongoing Identification of New Vulnerabilities
- Web Application Scanning
- Application Code Reviews
- Vulnerability Scanning
- Perimeter Security Monitoring (Firewalls, IDS/IPS)
- Log Monitoring/Log Retention
- Third-Party Risk Management
- Security and Risk Consulting

4. Validate Compliance

This phase involves performing the required PCI compliance assessments in the form of annual on-site PCI assessment and quarterly PCI network scanning. As a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), Dell SecureWorks can assess organizations current state of compliance, assist in their remediation efforts and create formal reports or observations of compliance.

Annual Onsite PCI Assessment

As a QSA, Dell SecureWorks is authorized to perform the required annual on-site PCI compliance assessment. At the completion of the assessment, Dell SecureWorks will provide recommendations and remediation plans for areas that fall short. Once remediation has taken place, Dell SecureWorks will re-assess the implemented controls. Once all requirements are properly met, Dell SecureWorks can issue an Attestation of Compliance or Report on Compliance.

Quarterly PCI Scanning

Merchants that have externally facing devices which interact with cardholder data are required to have quarterly vulnerability scans of all Internet-facing PCI-related systems. As an ASV, Dell SecureWorks can meet your quarterly scanning needs. Our PCI scanning service, powered by QualysGuard technology, performs highly accurate scans of your externally facing systems as required by PCI DSS, identifies active threats, and helps you remediate vulnerabilities detected in the scan. Our scanning engine is all managed through one easy to use online portal.

Security and Risk Consulting

Dell SecureWorks' Security and Risk Consulting professionals provide expertise and analysis to help you improve your security posture, facilitate compliance and improve operational efficiency. With deep experience in PCI compliance as well as ISO, NIST, HIPAA, GLBA, and other standards, our security experts identify risks and prepare you for a favorable assessment of your IT controls.

Our consulting services deliver:

- Actionable information to improve your security
- Clear, concise reports to demonstrate compliance
- A team of experienced security professionals to analyze your environment.

About Dell SecureWorks

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.

For more information,
call 877-838-7947 to speak to a
Dell SecureWorks security specialist.

www.secureworks.com

SecureWorks