

PCI SOLUTIONS

The PCI Data Security Standard

Driven by increasing identity theft and weekly headlines about data breaches at some of the biggest corporations, the payment card industry (PCI) created standards to enhance the security controls protecting card data from theft and misuse. Developed by major payment brands which had their own individual programs for card data protection, the PCI Data Security Standard (PCI DSS) enables broad adoption and enforcement of consistent security measures across all merchants and service providers that touch card data.

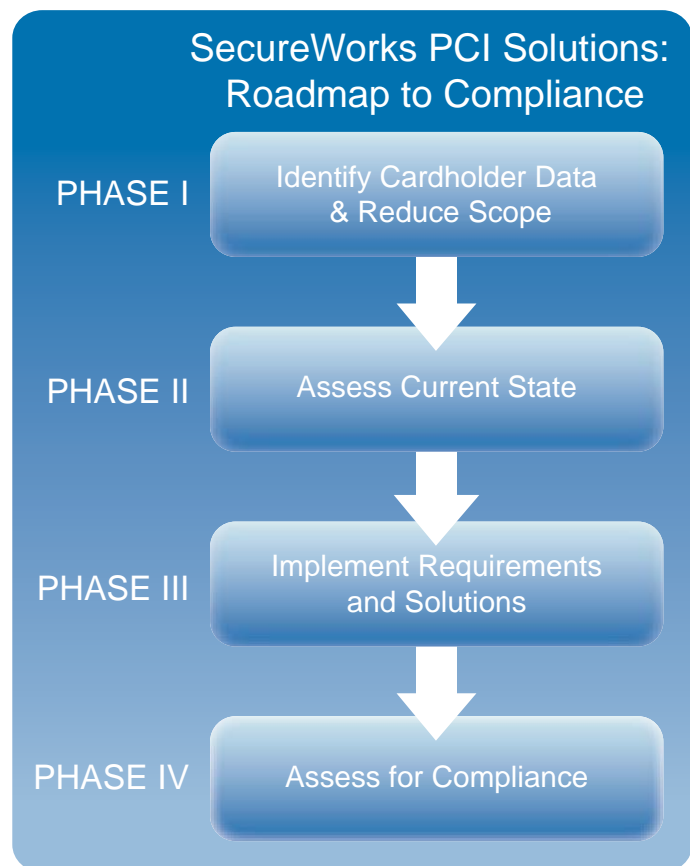
Intended to create an additional level of protection for customers and reduce the risk of data breaches involving personal cardholder data, the PCI DSS requires any organization that processes, stores or transmits credit card data to meet minimum levels of security or face stiff penalties. Enforced by card issuers, non-compliance with the PCI DSS requirements can have a devastating impact on merchants and financial institutions.

For example, a large breach at CardSystems Solutions involving the theft of 40 million credit card account numbers ended with the company shutting down and closing its doors. After the post-breach on-site PCI audit found CardSystems to be non-compliant, Visa and American Express dropped the company as a card processor and CardSystems was forced out of business.

The PCI DSS version 1.2 is comprised of 12 broad requirements which organizations must meet each year to maintain compliance. 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.

SecureWorks PCI Compliance Solutions

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



SecureWorks uses a four-phase roadmap to assist businesses in their PCI compliance efforts.

PCI SOLUTIONS

Phase I: 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 card-holder data, this phase focuses on reducing what is considered in-scope for PCI DSS in order to minimize “wasted motion” and reduce costs.

Data Flow Analysis

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

Mapping Cardholder Data

Through interviews, document review, network review and data searches across the network, 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, SecureWorks identifies and designs the best network architecture to consolidate where cardholder data is transacted, 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.

Scope Classification

Based on interviews and analysis, SecureWorks accurately determines what level of scope an organization is subject to for PCI DSS. This involves determining whether the organization falls into one or more of the following categories:

Merchant - Level 1, 2, 3, or 4

Service Provider - Level 1, 2, or 3

Once classified, SecureWorks identifies the requirements that must be met in order for the organization to prove compliance.

Phase II: Assess Current State

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

PCI Gap Analysis

SecureWorks assesses an organization’s current environment against the Data Security Standards using a combination of the DSS, the DSS Audit Procedures and the Self-Assessment Questionnaire. This identifies where gaps and opportunities for improvement exist as compared to the DSS requirements.

Self-Assessment Questionnaire (SAQ) Assistance

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. In the event of a breach or on-site PCI audit, this document could be used as a basis for further investigation. Making sure the SAQ is accurate and complete is critical.

Develop Remediation Plans

At the completion of the Gap Analysis or SAQ, SecureWorks can develop detailed plans for remediation that are designed to meet the DSS requirements.

Assist in Remediation

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

PCI SOLUTIONS

Phase III: Implement Requirements and Solutions

This phase focuses on implementing solutions that help organizations meet specific DSS requirements. In some cases, this would be in the form of consulting services to develop specific policies or procedures. In others, it would involve performing consulting services to fulfill specific requirements such as penetration testing and web application assessments.

SecureWorks also provides Managed Security Services to meet other PCI DSS requirements.

Solutions include but are not limited to:

- Policy Development
- Development of System Configuration Standards
- Ongoing Identification of New Vulnerabilities
- Web Application Testing
- Application Code Reviews
- Penetration Testing
- Internal Vulnerability Scanning
- Perimeter Security (Firewalls, IDS/IPS)
- Log Monitoring

Phase IV: Assess for Compliance

This phase involves performing the required PCI compliance assessments in the form of annual PCI audits and quarterly PCI scanning. As a Qualified Security Assessor (QSA) and Authorized Scanning Vendor (ASV), SecureWorks can audit organizations for compliance, assist in their remediation efforts and submit all required paperwork to the proper parties.

As a Qualified Security Assessor (QSA) and Authorized Scanning Vendor (ASV), SecureWorks can audit organizations for PCI compliance, assist in remediation efforts and submit all the required paperwork to the proper parties.

Annual On-site PCI Audit/Report of Compliance

As a QSA, SecureWorks is authorized to perform the required annual on-site PCI compliance audits for Level 1 Merchants and Level 1-2 Service Providers. At the completion of the audit, SecureWorks will complete the Report of Compliance (ROC) or provide recommendations and remediation plans for those that fall short. Once remediation has taken place, SecureWorks will re-asses and complete the ROC at that point.

Quarterly PCI Scanning

All entities that fall under the PCI DSS are required to have quarterly vulnerability scans of all web-facing PCI-related systems. As an Authorized Scanning Vendor (ASV), SecureWorks can meet your quarterly scanning needs.

About SecureWorks

With over 2,000 clients, SecureWorks has become one of the fastest-growing Security as a Service (SaaS) providers safeguarding more organizations 24x7 than any other vendor. Positioned in the Leader's Quadrant in Gartner's Magic Quadrant for Managed Security Services Providers (MSSPs), SecureWorks is the only named leader that focuses exclusively on security services. SecureWorks protects our clients through our on-demand Security Management platform augmented with applied security research and GIAC-certified experts.

PROFESSIONAL SERVICES

Professional Services

SecureWorks Professional Services provide expertise and analysis to help you improve your security posture, facilitate compliance, and improve operational efficiency. With deep experience in GLBA, HIPAA, Sarbanes-Oxley, and NERC compliance, our security professionals identify risk and prepare you for a favorable exam of your IT controls.

Our Professional Services deliver:

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

“SecureWorks’ assessment of our systems was more accurate than our previous ones, they have a good structure for their audits, and we especially liked their exiting of the risk assessment with a presentation for management.”

Marshall Bissonnette, Systems Engineer
Big Rivers Electric Corporation

Compliance & Certification

Compliance: ISO 27001/17799, PCI, GLBA, HIPAA, NERC CIP, SOX
Equifax and Experian Certification

Program Development & Governance

Business Impact Analysis
Information Security Program Development
Policies, Standards and Security Baseline Development
Security Awareness Program Development and Training
Vendor Management Program Development
Merger and Acquisition IT Controls Diligence
Internal Audit Support

Incident Response Services

Response Planning & Analysis
Emergency Response
Incident Handling Services
Forensic Investigation
Malicious Code Analysis
Retainer Services
Phishing Takedown

Architecture

Enterprise Security Architecture and Standards Development
Identity and Access Management Architecture
Wireless and Mobility Architecture
Network Security Architecture

Testing & Assessments

Enterprise Risk Assessment
Vulnerability Assessment
Penetration Testing
Web Application Testing
Secure Code Audit
COBIT Assessment
Authentication and Authorization
Security Assessment
3rd Party Diligence
Wireless Assessment
Social Engineering
War Dialing