PCI DSS Compliance Services

Ensure PCI compliance by identifying vulnerabilities and gaps in how you store, process, or transmit payment and cardholder data

Many organizations face a significant investment in capital solutions and resources in order to comply with the PCI DSS requirements. The key is to avoid straining your information technology department to manage and remediate the vulnerabilities identified as part of the compliance process. Our Foundstone® Services experts understand PCI compliance and can help you navigate the complex and difficult-to-manage process.

The Payment Card Industry Data Security Standard (PCI DSS) was created to provide a set of common industry security requirements for service providers and merchants who store, process, or transmit cardholder data. Participating payment brands have agreed to mandate compliance with the PCI DSS for each of their data security compliance programs.

PCI Security Standards Council is responsible for qualifying and training Qualified Security Assessors (QSAs)—vendors qualified to conduct annual security assessments, and Approved Scanning Vendors (ASVs)—security solution providers who can execute quarterly vulnerability scans. Foundstone Services is both a qualified QSA and a qualified ASV. Both services are required to assess compliance with the PCI DSS.

Benefits

The PCI DSS often presents a serious challenge for most organizations to meet. Complying with the PCI DSS, however, can also render positive results in a number of key areas, including:

Protect damage to image and reputation. While the cost of fraudulent activities can usually be managed, the damage to an organization's image and reputation is difficult to overcome.

Prioritize information risks. Full compliance with PCI DSS requirements requires obtaining a full understanding of the technology-related issues and risks and prioritizing issues so resources can be allocated appropriately to ensure the security of cardholder information.

Increase comfort level with senior management. Becoming compliant helps assure senior management that proper security safeguards are implemented and the organization has met PCI requirements, allowing them to concentrate on other critical business issues.

Who Must Comply?

Any company that stores, processes, or transmits cardholder data must comply with the PCI requirements. This includes anyone from online stores, to small mom-and-pop shops, to large corporations.

Most consumers do not concern themselves with the lifecycle of a credit card transaction. Many believe the transaction only exists between the merchant and the bank. Although this notion is partly correct, there can be several other entities involved in the transaction, which increases the risk of exposure.

The Foundstone Services Approach

The objective of the PCI DSS is to achieve a common minimum security level that protects cardholder information. If any of the requirements have not been satisfied, the card brands may require additional information, such as a remediation plan for becoming compliant and associated timelines. As a qualified QSA and ASV, Foundstone Services has developed a measured approach to help steer organizations towards compliance.

Foundstone's approach consists of six services:

Data flow analysis

We start by mapping and identifying where cardholder data is stored and/or processed. Data is traced and mapped from a card swipe or user input on a web server, down to the payment acquirer. Knowing where cardholder data resides provides an accurate scope for compliance requirements. During this phase, devices, systems, and applications that store, process, or transmit cardholder data are recorded. Data flows are critical to designing appropriate remediation steps for any gaps identified during the next phase.

Network architecture review

This service is used to understand the placement of the devices, systems, and applications that store, process, or transmit cardholder data. We identify opportunities to isolate these systems from the rest of the network, restricting the exposure of cardholder data and related devices, systems, and applications to other non-PCI systems. Doing so not only improves the overall security of the cardholder data, but also allows you to reduce the scope of systems covered by PCI, and thereby optimize the resources required to achieve compliance.

Preliminary gap analysis

This helps you understand the environment, to identify controls in place, and to carefully map the environment to each of the twelve PCI DSS requirements of the controls. We review policy and procedures documentation, interview key employees, assess device configurations, and verify compliance with policies and review of physical security. The main objective is to identify any gaps and vulnerabilities which might exist.

Network vulnerability scanning and penetration testing

We execute external network vulnerability scans on a client network, validating the scan results and performing a penetration test on systems and applications. Network vulnerability scanning utilizes a scan solution that automatically scans a range of network addresses and performs numerous tests to detect vulnerabilities in specific network services. The service identifies any well-known vulnerabilities associated to that system. Penetration testing leverages the experience of Foundstone consultants to identify other subtle yet serious vulnerabilities that cannot be identified by network vulnerability scans.

Remediation planning and road map

This service consists of developing solutions and planning a road map to assist with compliance. With immediate actionable tactical steps that bridge identified gaps, to strategic projects and foundation changes, a roadmap will be developed with actionable plans that meet both business and compliance needs today and in the coming years.

Report on compliance (ROC)

The ROC is the result of assessing the client's environment based on the PCI requirements and generating a compliance report. The report is constructed based on PCI guidelines and a copy of the report is distributed to the client, the acquirer, and payment card association.

The Foundstone Difference

The Foundstone Services team has a long history of working with clients across the globe, both as a technology partner to support our anti-malware, antispyware, and antivirus software solutions and also as a strategic advisor with product-agnostic, program-level engagements. Our teams of security experts assess network vulnerabilities, evaluate gaps in information security programs, offer strategies that meet compliance goals, and even help develop programs to prepare for security emergencies.

Learn More

We provide security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about our services or email us at **foundstone@mcafee.com**.

Get more information at **www.foundstone.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com