PAYMENT CARD INDUSTRY COMPLIANCE SERVICES

PCI SERVICES

Key to consumer confidence. Economic stability. Business security. And growth.

The PCI Security Standards Council (PCI SSC) is an open global forum launched in 2004 to develop, maintain, and manage standards for credit card merchants and payment applications.

Their Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all organizations that process, store, or transmit credit card information maintain a secure environment.

WHO MUST MEET PCI COMPLIANCE?

PCI standards apply to *all* organizations or merchants that accept, transmit, or store any cardholder data—*regardless of size or number of transactions.*

WHAT IS REQUIRED TO BE PCI COMPLIANT?

There are four levels of compliance requirements, based on the volume of transactions.

All merchants are required to be compliant with the PCI DSS, which includes regular monitoring and testing of their networks. Level 1 and 2 merchants processing greater than $1M (or others if requested by the payment card issuer) are subject to annual audits by a Qualified Security Assessor (QSA). In addition, any merchant with e-commerce must also complete a vulnerability scan by an Approved Scanning Vendor (ASV).

FORESITE PCI SERVICES HIGHLIGHTS

- Expert advice and guidance to understand and meet PCI requirements
- Scoping assessments to ensure proper segmentation to minimize PCI costs and risks
- Gap assessments to review network architecture and controls to identify impediments for successful audits
- ASV scanning / penetration testing
- Internal /external vulnerability scans
- Thorough audit against current PCI DSS by team of Qualified Security Assessors (QSAs)
- Report on Compliance (ROC)
- Attestation of Compliance (AOC)

PCI DATA SECURITY STANDARD High Level Overview

Build and maintain secure network	1. Install and maintain 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 vulnerability management program	5. Use and regularly update anti-virus 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. Assign unique ID to each person with computer access 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 information security policy	12. Maintain policy that addresses information security for all personnel

INTELLIGENCE. DIRECTION. ATTENTION. LEADERSHIP.

Level of compliance and the applicable PCI standards are often confusing to organizations and leave them guessing. Do their processes and controls meet the standards? And, even more importantly, what falls under the scope of PCI? For example, if an organization has only one or two credit card terminals, but its network includes multiple locations with virtual servers, is the whole network in scope?

Foresite can find the answers. Our process begins with a scope and gap assessment of your business to determine proper network segmentation for effectively and efficiently managing what is in scope for your PCI audit. We then review your network architecture and controls and provide feedback on problem areas to prepare you for a successful audit.

We also perform a thorough audit of your business against the current PCI DSS protocol and provide you with a Report on Compliance (ROC) and Attestation of Compliance (AOC).

Note that if you are an organization that develops software or integrates payment applications that store, process, or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties, you are also required to adhere to the Payment Application Security Standard (PA-DSS).

Foresite is one of only a few companies in the world that is both a Qualified Security Assessment Company (QSAC) and a Payment Application Qualified Security Assessment Company (PA-QSAC). That makes us leading, qualified experts in meeting the requirements of all your Payment Card Industry Data Security (PCI DSS) and Payment Application (PA-DSS) Standards initiatives.

MEET YOUR PCI MONITORING REQUIREMENTS

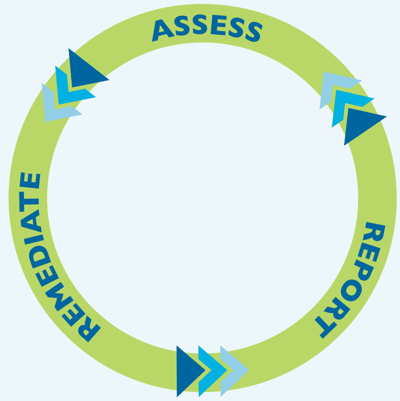
LOG MONITORING, ANALYSIS & ALERT MANAGEMENT

Enterprises can generate millions of log alerts every day–making the recognition and analysis of meaningful alerts in real-time a complicated, resource-consuming challenge.

Today, security teams already struggle to stay focused on simply managing resource bandwidth. Today, there's a solution that can put you in control.

Foresite security monitoring solutions, managed by our team of certified security analysts, offer the focus and expertise required to meet your objectives–in place, on point, 24x7. That means peace of mind. And the time and resources to concentrate on your business goals.

PCI IS A CONTINUOUS PROCESS



PCI Security Standards Council®

QUALIFIED SECURITY ASSESSOR™

FORESITE

VISIONARY IT SERVICES

Founded in 1997, Foresite is the go-to provider of information security and network solutions for hundreds of companies—and is now emerging as the preeminent source for managed security and cloud solutions. Our solutions address the liabilities of today's complex security and compliance requirements. Our long-experienced professionals apply their expertise to providing superior product performance and unparalleled customer service through Foresite's proprietary ProVision platform. Headquartered in Overland Park, Kansas, Foresite has operations centers in Rocky Hill, Connecticut, and London.