



PCI Compliance Program & Solutions Suite

THE PROBLEM OVERVIEW

Addressing PCI Compliance requirements can be a daunting task when a merchant must do the following:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a Vulnerability Management Program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an Information Security Policy

THE PERIMETER PAYMENT CARD INDUSTRY (PCI) COMPLIANCE PROGRAM

The Perimeter Payment Card Industry (PCI) compliance program has been designed to help meet PCI-DSS regulations, which requires members, merchants and Service Providers of the PCI network to proactively protect themselves and the overall payment system against the threat of Internet based vulnerabilities. These vulnerabilities create weaknesses that could lead to the exposure of private information, theft of intellectual property, customer identity theft, violation of privacy laws, extensive brand damage and potential litigation. Our program helps satisfy the external component of the PCI certification by identifying vulnerabilities in security processes, procedures and web site configurations.

Perimeter's PCI Compliance Program includes two services that address the base requirements of a merchant:

1. NETWORK VULNERABILITY SCANNING

Your external network is scanned from Perimeter's Security Operations Center to give a true picture of your organization's external exposure. Results from the assessment are reported to management and IT administrators to provide a clear picture of your network's current vulnerability status. All reports are presented in the certified PCI compliant format to adhere to industry certification requirements. The reports include complete analysis and remediation recommendations, along with an overall compliance grade.

2. SELF ASSESSMENT QUESTIONNAIRE

In addition to the PCI scanning requirements, merchants must also complete one of four self assessment questionnaires that measure compliance with the PCI council's data security standard. To help customers complete their requirement, we offer an advanced service which includes an annual conference call where a qualified CISSP security consultant will help facilitate the successful completion of the questionnaire.



Complete. On Demand. Affordable.

THE PERIMETER PCI SOLUTIONS SUITE

Most vendors who offer PCI compliance services include external vulnerability assessments and questionnaire assistance, but how can you ensure that you'll pass your assessment? What happens if you don't? Can you turn to that same provider to satisfy all of your regulatory needs? With Perimeter you can. The Perimeter PCI Solutions Suite consists of two levels of services designed specifically to satisfy PCI requirements. No other provider can offer your organization so many services to help satisfy all of your PCI regulatory needs.

PRIMARY PCI SERVICES

Perimeter's Primary PCI Services have been specifically mapped to PCI-DSS regulations. These services offer your organization the broadest amount of coverage from a risk mitigation standpoint. These are technologies that are specifically called out in the regulation (or sub-component of the regulation) and are necessary for all merchants to have.

PRIMARY SOLUTIONS	DESCRIPTION
Firewall & Intrusion Detection	Perimeter will monitor your firewall 24 hours a day, seven days a week from our Security Operations Center
System Anti-Virus	Fully managed anti-virus software, automatically updating anti-virus clients on desktop computers and servers
Monthly Remote Network Assessment (Internal, External, & Policy)	Provides a range of vulnerability scanning, testing, and reporting services for clients that want to manage both their internal and external network vulnerabilities and exposure
Patch Management	Fully automate your organization's vulnerability detection and patching needs by proactively downloading patches from all major software vendors
eSecurity Training	Easy-to-use, fully customizable and brandable online training course to ensure that employees are trained on the same material in the same manner

SECONDARY PCI SERVICES

Perimeter's Secondary PCI Services have been chosen because they are necessary for most merchants, but not all. They are all considered to be essential to a quality, layered security solution.

SECONDARY SOLUTIONS	DESCRIPTION
Remote Data Backup & Recovery	Securely encrypts, backs up and recovers critical business files in a secure, off-site Level 3 data storage center
Virtual Private Network	Remote users can access a network connection that establishes a secure IPSec tunnel across the Internet to take them to work on your network
MailSafe Encrypted Email	Allows users to send electronic messages securely to anyone on the internet through a secure, encrypted channel
User Access Auditing	A reliable, proactive and practical enterprise class solution to centrally monitor and analyze critical system access records which are stored within Windows NT/2K/XP/2003, Novell Netware and Linux server SYSLOGs