Conformance™

WHITE PAPER

NEW PCI DSS REQUIREMENT
PENETRATION TESTING AND CREDIT CARD SCANNING

Tougher Penetration testing (Pentesting) requirements, mandated by the Payment Card Industry Data Security Standard (PCI DSS) became effective July 1, 2015. Merchants must validate if credit card data is stored and if transaction processing systems are safe from malicious hacker attacks.

Without the proper third-party tests, merchants are non-compliant and risk data breaches, fines and increased costs.

Many merchants confuse penetration testing, vulnerability scanning and credit card (PAN) scanning.

What is Vulnerability Scanning?

Vulnerability scanning is a fully automated process that identifies potential security gaps used by hackers to attack systems. PCI DSS requires quarterly vulnerability scanning as a part of an overall security compliance program.

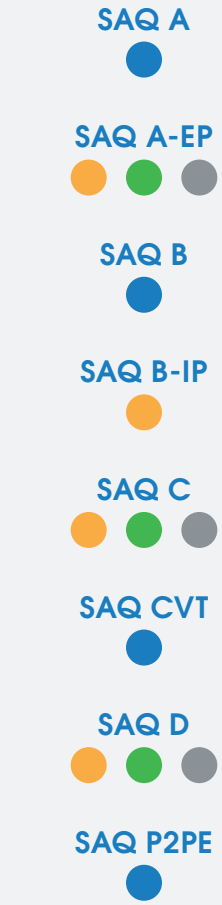
What is Penetration Testing?

Pentesting is an in-depth test performed by security professionals using same techniques hackers use. Mimicking real-world attacks to test security systems is an advanced security testing technique that must be conducted on an annual basis, and after any major changes to the computing environment.

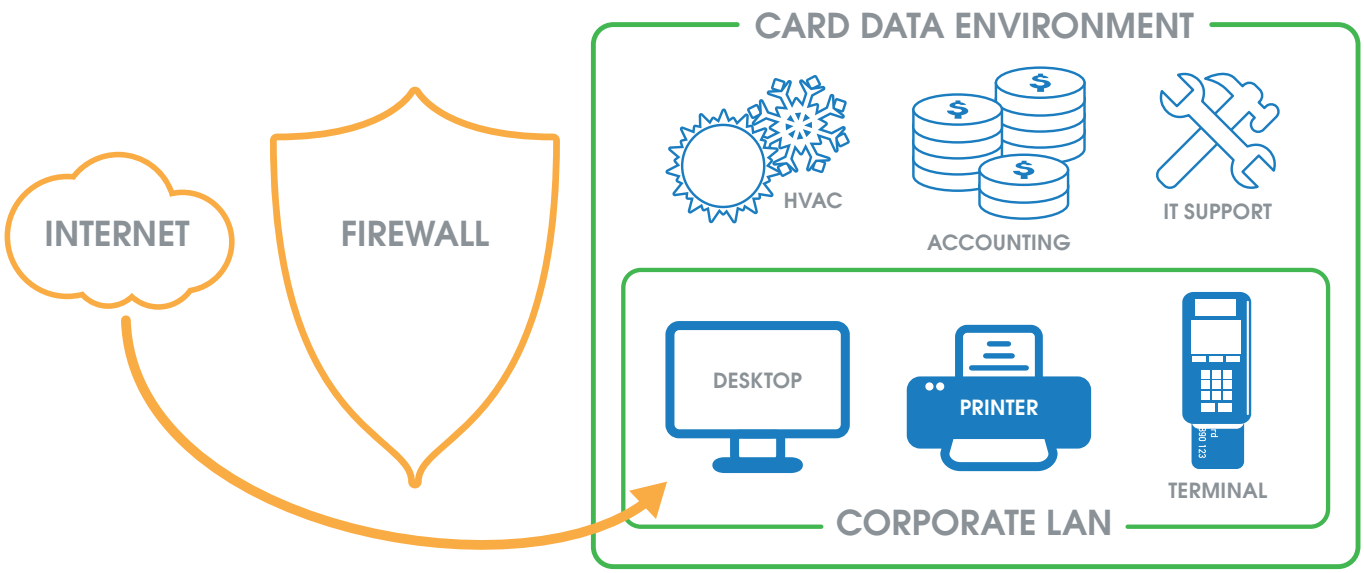
What is PAN Scanning?

PAN scanning for Primary Account Numbers (PAN or credit card numbers) and track data is recommended as a method to ensure that sensitive data is not inadvertently stored in payment systems. PAN information may not be stored by merchants unless protected by strong cryptography. Many merchant systems have the potential to generate error logs, transaction records and other output that includes full, unencrypted credit card numbers, without their knowledge or consent! Without regular PAN scanning, merchants expose their business to a greater risk of data breach consequences.

WHAT MERCHANTS NEED



Vulnerability Scanning, Pentesting and PAN Scanning Flow



Why Merchants Need Vulnerability Scanning, Pentesting and PAN Scanning?

PCI DSS requires Pentesting, not only for e-commerce merchants, but for some brick-and-mortar merchants as well. It is generally accepted by industry experts that Vulnerability Scanning and PAN Scanning are critical components and requirements of a complete penetration testing exercise. Fines and sanctions for exposed card data can and do run into the tens of thousands of dollars. It's important to begin protecting your business today.

Unfortunately, a complete security assessment firm exercise, involving Vulnerability Scanning, Pentesting and PAN Scanning, typically costs $5,000 - $10,000 depending on system complexity, and frequently takes weeks to complete.

Conformance Technologies Can Help!

Conformance Technologies' Cyber Attack Readiness ToolKit™ provides comprehensive Vulnerability Scanning, Pentesting and PAN Scanning services, with the same quality and effort as security assessment firms, but at 80 - 90 percent LESS cost. Scans and tests can be performed as often as you like with no upfront expense using our monthly subscription service.

In addition to complying with PCI DSS requirements, the Cyber Attack Readiness ToolKit identifies system vulnerabilities nearly 100 percent of the time, plus 94 percent of examinations identify unsecured credit card data.

The Cyber Attack Readiness ToolKit is easy to use. As soon as you enter the IP addresses associated with your systems, our testing engine and security engineers begin vulnerability checking. NO CONFIDENTIAL DATA leaves your system! Testing communicates areas of vulnerability, not data. In just a few short days, recommended actions and status reporting is available for review online. Plus, security engineer support is provided at no additional cost.

Conformance™

To learn more about the Cyber Attack Readiness ToolKit and other sensitive data solutions built on the Conformance Compliance Operating System™, please call 775.336.5533 or visit us at conformancetech.com.

Conformance Technologies ○ 2780 S. Jones Boulevard, Suite 3796, Las Vegas, NV 89146 ○ 775.336.5533 ○ conformancetech.com ○ V091315