

## Key Reasons To Choose netVigilance PCI

- » Achieve PCI compliant status and secure your network
- » Detect up to 97% of common vulnerabilities, with the fewest false-positives of any solution
- » Minimize risk + maximize value by using the only solution that goes Beyond Compliance™
- » Unlimited number of URLs included
- » New PCI ASV Program Guide V1.0 requirement: Every report always validated by a PCI Qualified Security Engineer
- » Determine whether intrusion detection systems are blocking the scans from being executed (a violation of PCI rules)
- » No software to deploy or maintain
- » Get highly detailed remediation instructions that quickly allow you to eliminate identified security threats



APPROVED SCANNING  
VENDOR  
#3757-01-04



# netVigilance PCI-DSS ASV Scans

Go Beyond Compliance™ with netVigilance PCI

**Fact:** 74% of data breaches in 2008 resulted from external sources, 32% from business partners, and only 20% from insiders (results add up to more than 100% because some had multiple causes).

**Fact:** 64% of breaches were attributed to hackers who used a combination of attack methods. 19% of breached organizations in 2008 were PCI-DSS compliant.

### PCI-DSS Background

Visa, MasterCard, American Express, Discover and the Japan Credit Bureau worked together to create a standard that held all retail (i.e., credit-card processing) merchants to certain minimum requirements for information security. The resulting standard was called PCI-DSS, for the Payment Card Industry Data Security Standard. Compliance with PCI-DSS ensures that consumers and shoppers know that any merchant who accepts their credit card also takes measures to ensure the privacy, protection and security of their personal credit card information. Merchants are required to have an Approved Scanning Vendor (ASV) test and certify them as PCI-DSS compliant. PCI-DSS ASV Scans cover both infrastructure and web applications, and they result in a special report that details the findings.

### netVigilance — PCI-DSS Approved Scanning

As an Approved Scanning Vendor (ASV), we are fully certified to assess PCI compliance. Our assessments go above and Beyond Compliance for global businesses, merchants and retailers, with:

- A well-documented, fast, easy, reliable way to achieve PCI compliance that protects cardholder information and mitigates your risks – with all required PCI validation reports and proof of compliance provided
- Infrastructure scans of critical network components that cover 100% of all PCI-DSS requirements and up to 97% of all common vulnerabilities on the Internet, a breadth far more comprehensive than any competitor's. This breadth encompasses everything from Bugtraq to full SANS Top 20 coverage to OWASP to known vulnerabilities from all the major manufacturers
- Easy detection of non-compliant components validates key infrastructure risk areas
- Identification of vulnerabilities per the internationally recognized CVE standard, and rated per the CVSS 2.0 specification

- The assurance that comes from using netVigilance — the ASV that provides more updates and corrections to the NIST database of CVSS 2.0 scores than all other ASVs in the world combined

### Choose Our Total coverage Solution To Pass PCI-DSS 1.2 The First Time

- Unlimited, highly accurate, external network security scans
- Unlimited, highly accurate, internal network security scans
- Monthly web application scans that cover custom applications

### Industry-Best PCI-DSS Scan Details

Our PCI-DSS scan includes the following components and the PCI-mandated report:

#### 1. Infrastructure Network Security Scan

- Tests firewalls, routers, switches, etc.
- Tests web, mail and database servers
- Checks open ports and services
- Checks for Trojans, common worms and backdoors
- Continually updates and detects PCI-defined vulnerabilities

#### 2. Web Application Scan

For all web applications that must be secured to meet PCI requirements:

- Detects and specifies the hardest-to-find vulnerabilities in those applications
- Provides clear remediation instructions to fix those vulnerabilities, down to the precise URL and exact nature of the problem
- Works on custom built, customized in-house, or purchased web applications
- Spiders customer websites to ensure Total Coverage

(continued on next page)

## How We Achieve Up To 97% Coverage

- » We update continually, week-in and week-out, and even over holidays, because hackers never take a break.
- » We check against the entire OWASP Top 10.
- » Is up-to-date on the most recent and relevant vulnerabilities.
- » In our QA Lab, we reproduce environments with real systems to cover a large cross-section of the most common target systems on the Internet. We constantly add to this list.
- » Not only do we test against the latest versions of popular platforms, but also against older versions still in common use.
- » We even test against competing products as part of our regular QA to ensure absolute thoroughness and completeness.

### 2. Web Application Scan (continued)

- Tests for complete OWASP Top 10:
  - o A1 –Injection (SQL-Injection)
  - o A2 –Cross Site Scripting (XSS)
  - o A3 –Broken Authentication and Session Management
  - o A4 –Insecure Direct Object References
  - o A5 –Cross Site Request Forgery (CSRF)
  - o A6 –Security Misconfigurations (NEW in 2010)
  - o A7 –Failure to Restrict URL Access
  - o A8 –Unvalidated Redirects and Forwards (NEW in 2010)
  - o A9 –Insecure Cryptographic Storage
  - o A10 –Insufficient Transport Layer Protection

### 3. State-of-the-Art PCI Compliance Reports

- Automatic web-based report generation — simply login to our web interface and click on the report type you want — it will be automatically generated while you wait
- Save time and money by accurately identifying potential security breaches and recommending the best remediation strategy
- Executive Summary provides easy-to-read overview of compliance status on a host-by-host basis
- Includes the required manual validation performed by a netVigilance PCI qualified Security Engineer, per section 3.2 of the PCI Security Standards
- Fewest false positives in the industry
- Architecture prevents failed reports from being improperly changed to “Pass”

### The netVigilance Free PCI Rescan Warranty

Scan customers unable to produce a passing PCI ASV scan every quarter are deemed non-PCI Compliant — unless they remediate the identified problems and prove those problems have been fixed within 90 days of the last passing scan.

Equally important, customers who fall out of PCI Compliance because they cannot remediate within this official time-frame are in a much more serious situation — they then must pass the PCI ASV scan for four quarters in a row in order to become PCI Compliant again.

That’s why you must take all actions necessary to ensure you never fall out of PCI Compliance — otherwise, it will take you a minimum of four quarters to qualify again. As your partner, netVigilance wants to ensure this never happens to you.

### How The Warranty Works

An annual PCI subscription includes four scans within twelve months. Each of these scans is covered by the netVigilance Free PCI Rescan Warranty — if you fail a given scan, you are automatically entitled to one (1) free rescan, at absolutely zero cost. This enables you to verify that your vulnerabilities have been correctly remediated.

### How To Qualify

Qualifying is simple. Your free scan must apply to the identical IP scope as the scan that failed, and it must be run within thirty (30) days of the Quarterly PCI ASV Scan. Of course, if the free rescan still does not meet the PCI standard, a standard charge will apply to each additional scan until a “pass” has been achieved.

Fortunately, this situation should never occur if the full set of netVigilance vulnerability assessment tools is used. In fact, PCI has specific requirements, namely 6.6 and 11.2, which mandate the use of such tools. netVigilance’s industry-best remediation is designed to be used prior to running the mandated PCI-DSS ASV scan, in order to ensure that you will pass that scan the first time.

netVigilance, Inc.  
14525 SW Millikan Way #34423  
Beaverton, OR 97005

tel: 503-524-5758  
www.netvigilance.com

