

netVigilance Total Coverage™

Standard Compliance Is Not Enough

On July 24, 2009, web-hosting leader Network Solutions publicly reported that the credit card information of 573,928 individuals had been compromised over an almost 3-month period at 4,343 e-commerce sites, even though the company honestly believed it was safe and completely PCI Compliant. The Ponemon Institute also reported that, in the last 12 months, 85% of organizations experienced data breaches.

Key Advantages

- » Tests for and finds up to 97% of common vulnerabilities, far more than any competitor. We find the problems before the problems find you and inflict serious financial or public relations damage.
- » Provides you with first-class remediation instructions that eliminate research on your end, saving you up to tens of thousands of dollars per year.
- » Has an extremely low false positive rate. This is important because each false positive costs you time and money to investigate vulnerability that actually does not exist. False positives are one of the biggest problems with typical remediation, but with netVigilance, you can concentrate your resources on actual problems.

Going Beyond Compliance™ sets the new standard in vulnerability detection

Such breaches are epidemic because compliance standards such as PCI are intended to gain broad adoption and to raise the minimum standard for data security at credit card merchants. While these are noble and worthy causes, they only fulfill a few of the requirements for best practices in security.

It is not surprising that problems arise when compliance standards become substitutes for best practices, exposing even the most respected companies to high levels of unacceptable risk. The solution is to go Beyond Compliance with Total Coverage from netVigilance.

Encryption, antivirus & intrusion detection systems are no substitute for vulnerability detection

Encryption, antivirus and intrusion detection systems are all last lines of defense for use after your enemy is inside the door. That's because the purpose of these systems is not to prevent an attack, but to minimize the impact of attacks not already defeated or neutralized. netVigilance Total Coverage discovers and reports those critical vulnerabilities that help you stop the enemy before he gets in the door, and it identifies more of these than any other solution on the market.

Solution Overview

Total Coverage from netVigilance is the industry-best, most comprehensive vulnerability assessment available. Total Coverage finds your security holes before the bad guys do in all critical areas of your network:

- Publicly accessible components at the perimeter, including web servers, firewalls, routers, and mail servers
- Behind your firewall
- Inside your customer web applications

Deployment Options

To suit your specific requirements and to minimize your Total Cost of Ownership (TCO), netVigilance offers Total Coverage in three different ways:

Through the cloud. netVigilance fully supports the cloud computing model, making all of our functionality available via SaaS technology. System requirements: IE 6.x+ or Firefox 2.0+.

Through Windows-based software, with the option to use your own MS-SQL server. System requirements: Windows XP or Windows 2003 Server.

As an Appliance. netVigilance EasyBox is a dedicated appliance installed in your network which runs all of our tests, downloads updates, issues reports, and does it all automatically. System requirements: IE 6.x+ or Firefox 2.0+.

Key Features

- » Finds up to 97% of common vulnerabilities
- » Easiest to deploy and use
- » Fastest path to total security
- » Broad – scans all your IP addresses
- » Flexible enough for SMBs
- » Comprehensive enough for the largest enterprises
- » Scalable
- » Near zero maintenance cost with automated updating, running and reporting
- » User-friendly – reports that both IT and non-IT managers can understand
- » Weekly updates and enhancements
- » Special & urgent updates as frequently as needed – no need to wait for the weekly update

Ongoing Monitoring & Support

Hackers are constantly developing new techniques to penetrate Internet-accessible systems. The netVigilance Security Research Team utilizes numerous security resources, including white-hat and black-hat ones, to ensure that we have complete knowledge of the most relevant vulnerabilities. To detect all vulnerabilities and threats – whether at the perimeter, inside the network or in your web applications – Total Coverage is continually updated.

Focus on actual vulnerabilities, not false positives

False positives cost you time, labor and money – up to four hours and hundreds of dollars each. To go Beyond Compliance, netVigilance takes extra steps to absolutely minimize false positives. You get to concentrate your valuable resources on fixing actual vulnerabilities, not incorrectly reported ones.

About netVigilance

netVigilance is the fastest growing vulnerability detection and assessment company, because it goes Beyond Compliance to identify and detect up to 97% of common network vulnerabilities, far more than any competitor. Among security companies, only netVigilance:

- Focuses exclusively on solutions for Network Vulnerability Detection and Assessment, including PCI Compliance
- Automatically produces robust reports that describe how to fix discovered vulnerabilities, saving its customers tens of thousands of dollars per year in time and effort that competitive solutions require
- Has an extremely low false positive rate, enabling you to focus your resources on fixing actual vulnerabilities
- Is an active member of the PCI ASV Task Force and the CVSS SIG under first.org, where we are a leader in industry efforts to improve these key standards

netVigilance, Inc.

14525 SW Millikan Way #34423
Beaverton, OR 97005

tel: 503-524-5758

www.netvigilance.com

