

NetDiligence PCI Security Compliance Scan Testing

Network Vulnerability Scan testing provides valuable information that supports efficient patch management and other security measures that improve protection against Internet hacking. Moreover, compliance for the Visa/MasterCard supported Payment Card Industry (PCI) security standard requires scan testing. Level 1, 2, and 3 merchants are responsible for ensuring that a quarterly network scan is performed on their Internet-facing perimeter systems by a qualified independent scan vendor.

NetDiligence is certified by MasterCard to conduct required PCI scan testing. NetDiligence provides remote, non-intrusive vulnerability scans against networks, hosts, and applications.

For businesses and financial institutions looking for 'hands-on' analysis and understanding of how well their network is actually protected against prevalent threats and vulnerabilities, NetDiligence offers effective network vulnerability scanning services to test the efficacy of perimeter devices such as firewalls, DNS and web servers. This service will identify 6000+ vulnerabilities that hackers can exploit due to unpatched, non-hardened or misconfigured externally facing network servers and devices.

Using the safe, non-intrusive technology of QualysGuard, our scanning service gathers information on the existing features of your system and analyzes the known security risks associated with those features. This service will audit targeted system(s) for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about the network. The resulting color-coded report presents findings, estimates risk levels, and makes actionable recommendations on fixes for issues. Depending on your system, results can be in your hand within hours. The final report is designed for anyone to understand, providing easy-to-understand risk level assessments in addition to detailed technical information.

Some Key Features:

- The PCI scan will test against 6000+ potential security vulnerabilities that hackers can exploit. Scans and reports on vulnerabilities on all 65,536 network ports per device.
- Vulnerability definition database is updated daily by security experts.
- Accuracy of the scanner is a primary requirement in choosing a network security auditing solution. Components of accuracy involve the depth and quality of the audits in combination with a vendor's ability to eliminate false-positives. QualysGuard leads the industry in scanning accuracy, delivering 99.997% overall accuracy (.003% false-positive rate)
- Fingerprints over 500 unique applications, operating systems and protocols
- REPORT: A clear and concise customized executive-level summary report is generated.

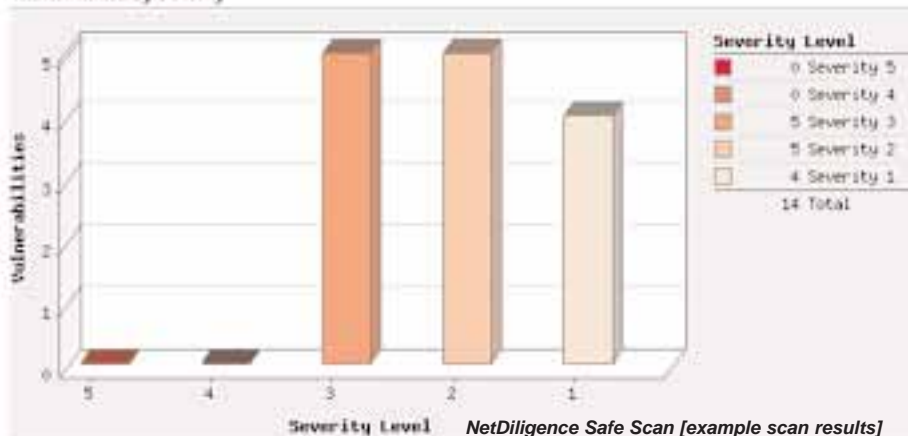


For PCI Scan All:

- Filtering devices (firewalls)
- Webservers
- Application Servers
- Web Applications
- DNS
- Mail
- Load Balancers
- Virtual Hosts (3rd party)
- Wireless APs

Contact Us Today!
1-610-525-6383

Vulnerabilities by Severity



Operating Systems Detected



REPORT Details: The NetDiligence PCI Scan produces a clear and concise executive-level report. The report details findings and illuminates outcomes graphically, prioritized by the threat severity and offers critical fix recommendations to remediate any vulnerabilities identified. The findings report also includes detailed descriptions of said vulnerabilities, and states upfront if compliance is achieved. To be considered PCI compliant, a scan must not contain high-level vulnerabilities. In the below example, this translates into vulnerabilities designated as level 3, 4 or 5.

Level	Severity	Description
5	Urgent	Trojan Horses, file read and writes exploit, remote command execution
4	Critical	Potential Trojan Horses, file read exploit
3	High	Limited exploit of read, directory browsing and denial of service (DoS)
2	Medium	Sensitive information can be obtained by hackers on configuration
1	Low	Information can be obtained by hackers on configuration