



The Importance of Using an ASV to Scan Your Network

An Overview of Approved Scan Vendors

Why is using an ASV to scan my network important? There is a lot of confusion out there regarding what vulnerability scanning is and why someone should pay the money to use a Payment Card Industry Security Standards Council (PCI SSC) Approved Scan Vendor (ASV) to do that scanning. In this paper I will dispel some of the misinformation and explain in layperson terms why using an ASV is important by answering some basic questions:

- What is a vulnerability scan?
- How does an ASV differ from a “regular” scan?
- How does this help me?
- What happens if I don’t scan my networks?
- Are there best practices for scanning?
- What are the regulator implications of not scanning NPI¹ / Card Data environment?
- Does scanning my network guarantee that I will not be hacked?

Should my explanation fail to impress upon you the importance of using an ASV to monitor the state of your networks security, I will have to revert to the old standby — you can’t be deemed compliant with the industry mandates and federal requirements unless you are using an ASV to scan your external IPs and are scanning your internal IPs for vulnerabilities on a regular basis (PCI DSS Requirement 11.2).

Now let’s get back to talking about the value that vulnerability scanning brings to your organization.

¹ The term "nonpublic personal information" means personally identifiable financial information (i) provided by a consumer to a financial institution (ii) resulting from any transaction with the consumer or any service performed for the consumer; or(iii) otherwise obtained by the financial institution.

Note: Such term does not include publicly available information.



What is a vulnerability scan?

A vulnerability scan is an automated process that proactively identifies vulnerabilities associated with the computing systems within a network in order to determine if and where a system can be exploited. These scans can be run on both internally- and externally-facing portions of the network. However, it is especially important that they be executed on public-facing servers as that is the area with the most potential for exploitation by threat agents, such as malicious hackers.

Vulnerability scanning solutions employ software that seeks out security flaws based on a database of known flaws. This software tests systems for the occurrence of these flaws and generates a report of the findings that can be used to tighten a network's security.

How does an ASV differ from a "regular" scan?

PCI Security Standards Council ASVs must undergo a certification process that is managed by the [Council](#). This process consists of using a "test bed" to validate that the scan vendor's solution is:

- Up to date
- Accurate
- Not too intrusive
- Non destructive
- Providing sufficient reporting (including remediation assistance)
- Meeting the level of vulnerability identification as set by the PCI SSC

This doesn't mean all ASVs are the same. It just means that they have demonstrated that they meet the standard the PCI SSC has established for the program. It should also be noted that ASVs are subject to the PCI SSC Quality Assurance Program which looks at the ASV internal operations. All this is a fancy way of saying that a PCI SSC ASV (say that 10 times fast!) has been independently reviewed and found to pass muster, so they are probably better than a solution that hasn't undergone another level of scrutiny.

(If this explanation does not work, please refer back to my comment about PCI SSC Requirement 11.2.)

How does this help me?

If you are able to find an issue with your network's security and fix it before the threat agent (read "bad people") does, you have saved yourself the expense and heartache that comes with an information security incident. Also, if you have hired someone to maintain your network for you, looking at the monthly ASV report could help you validate that they keeping up with system patches and keeping your network secure (now that's just good vendor management!).

What happens if I don't scan my network?

Is an ostrich safer from a predator when it has its head in the sand or when it sees the predator coming (remember, those suckers can run 45MPH!)? My point is that not scanning is the equivalent of putting your head in the sand. Assuming your network is secure doesn't assure that it is. It is always best to run the scans and be certain.



Also, at the risk of being repetitive, if you have Cardholder Data or Non-Public Person Information (NPI) you are required by contract (merchant agreement) and by law ([GLBA](#), [Minnesota Plastic Card Security Act](#), [HIPAA Htech](#)) to secure your network. Vulnerability scanning is a required component of that law (more on that later).

Are there best practices for scanning?

According to the best security practices unit of the [Yankee Group Research Inc.](#), a Boston-based technology advisory firm, organizations should perform vulnerability management on at least a daily or weekly basis.

If you are a PCI DSS level 1 – 3 merchant, you are required to file a “compliant” ASV report on a quarterly basis and sometimes it can take a few weeks to resolve the issue, so a monthly scanning regimen should be the minimum an organization should consider.

What are the regulatory implications of not scanning my NPI / card data environment?

If you are a merchant, tax accountant, attorney (Refer to the IRS [Publication 3112](#)), or financial institution, the result of non-compliance is the same (legal fees, non-compliance assessments, regulatory actions), so compliance with the PCI DSS scanning requirement is a must.

Does scanning my network guarantee that I will not be hacked?

The answer to this question is a resounding **NO!** However, time and time again forensic studies show that it isn't brand new system vulnerabilities (called “0 day” vulnerabilities) that are being exploited, it is the known vulnerability that has been on the network 30, 60, 90+ days that has a readily available fix that is used to exploit most systems. So, use of a tool that keeps up with known system vulnerabilities and provides direction on how to resolve them (as ASVs are required to do), will greatly reduce the probability of you being hacked... We will address the value of monitoring your audit logs at another time.

***Jim Bibles** leads the Business and Product Development teams for ComplyGuard Networks. He is widely recognized as an expert in the development and implementation of risk-based compliance programs. His focus for the past 10 years has been in the payment space where he has implemented information security and merchant PCI DSS compliance programs for such companies as Visa Inc. and Wells Fargo Merchants Services. His current focus is developing merchant network vulnerability and risk management tools for small to medium-sized businesses and their service providers, so that they are in a better position to make intelligent, risk-based decisions on how they secure their network. Jim is a QSA and is an active thought leader within the payments community.*

About ComplyGuard Networks

ComplyGuard Networks has more than 30 years of combined expertise in network security including vulnerability assessments, audit, penetration testing, and web application security. Our intellectual property portfolio positions ComplyGuard Networks uniquely in statutory and policy compliance. ComplyGuard Networks can provide any PCI or network security-related services businesses may require. For more information, contact us at 210-835-2000 or email info@complyguardnetworks.com. On the Web, visit www.complyguardnetworks.com.

Copyright © 2011 ComplyGuard Networks

