Vulnerability Assessment Scanning

Why Sunbelt Network Security Inspector (SNSI)?

Sunbelt Software White Paper
February 2004
Executive Summary:

Vulnerability assessment is an important element of a comprehensive multi-layered system and network security plan. Vulnerability assessment scanners can simulate the actions of hackers and attackers and check system settings to help administrators pinpoint security weaknesses before they are discovered – and exploited – by outsiders. Such tools can remotely assess the secure status of your network (or the lack thereof) and generate reports documenting scan results that you can use as a guide to fixing the identified problems.

There are dozens of vulnerability assessment scanners on the market, and sorting through the different technologies (network based, host based, agent-based, client/server), different features, different reporting methods, and different licensing schemes is a challenge. The number and accuracy of vulnerability checks differs widely from one product to another, as does the usability of the reports generated. Selecting the right tool is the most important factor in determining whether the addition of a vulnerability scanner to your security arsenal is worth the cost.
Table of Contents:

Vulnerability Assessment Scanners: What They Are and What They Do.............................. 4
Find Security Holes Before They Become Problems ........................................................... 4
Proactive vs. reactive security .............................................................................................. 5
Vulnerability Assessment Scanning Hacks Your Network – Before a Hacker Does .......... 5
Importance of Vulnerability Assessment to Network Security ............................................ 6
How Vulnerability Assessment Fits into your Multi-Layered Security Plan .................... 7
How a Comprehensive Security Plan Gives Your Company a Competitive Edge ........ 7
Vulnerability Assessment Technologies: How They Work .................................................. 8
Underlying Technology ........................................................................................................ 8
Features Administrators Want ............................................................................................. 9
Vulnerabilities database ....................................................................................................... 9
Ease of Use .......................................................................................................................... 10
Reporting ............................................................................................................................. 10
Analysis and Recommendations ......................................................................................... 10
Accuracy of analysis ............................................................................................................ 10
Security Issues .................................................................................................................... 11
Performance ........................................................................................................................ 11
Vulnerability Assessment Scanner Pricing Structures ....................................................... 11
Per IP Block ......................................................................................................................... 11
Per Server ............................................................................................................................ 12
Per Administrator ................................................................................................................ 12
Who’s Using Vulnerability Assessment and What Are They Using? ............................... 12
Who’s Not Using Vulnerability Assessment Scanners – and Why .................................. 12
Cost factors ........................................................................................................................ 13
Time factors ......................................................................................................................... 13
The “It Won’t Happen to Us” Factor .................................................................................. 13
Consequences of Security Breaches .................................................................................. 13
Direct financial loss ............................................................................................................ 14
Cost of downtime in productivity ....................................................................................... 14
Lost future business: the “ripple effect” .......................................................................... 14
Litigation/legal factors ....................................................................................................... 14
Why SNSI is the Best Choice for your Vulnerability Assessment Needs ......................... 14
How SNSI Addresses the Problems That Prevent Companies from Using Vulnerability
Scanners .............................................................................................................................. 14
How SNSI Prevents the Consequences of Security Breaches .......................................... 15
How SNSI Pricing Structure Saves your Company Money .............................................. 15
Summary .............................................................................................................................. 15
REFERENCES ....................................................................................................................... 16

Why Sunbelt Network Security Inspector?
Page 3 of 16
Vulnerability Assessment Scanners: What They Are and What They Do

The dictionary defines *vulnerability* as weakness or lack of adequate protection. In military terminology, the meaning is more specific – and more ominous: *open to attack*. Every system has vulnerabilities; only Superman claims to be invulnerable (and even he shows his weakness when Kryptonite is around). Regardless of the steps you’ve taken and the money you’ve spent to implement security, your network almost certainly still has characteristics and configurations that an attacker could exploit. That’s the bad news.

The good news is that most attackers, like most people in general, like to do things the easy way. And it’s easier to exploit known vulnerabilities than to discover brand new ones. That means the majority of attacks will be aimed at the common security “holes” in operating systems or applications that have already been documented.

Why is that good news? Because, with the proper tools, it’s just as easy for businesses to find the weak points in their own networks as it is for hackers to find them. Then you can do something about them. But how to find them – quickly and easily – is the key, and that’s where vulnerability assessment scanners such as Sunbelt Network Security Inspector (SNSI) come in.

Find Security Holes Before They Become Problems

Vulnerabilities can be classified into two major categories:

- Those related to errors made by programmers in writing the code for the software.
- Those related to misconfigurations of the software’s settings that leave systems less secure than they could be (improperly secured accounts, running of unneeded services, etc.).

Vulnerability scanners can identify both types. Vulnerability assessment tools have been around for many years. They’ve been used by network administrators and misused by hackers to discover exploitable vulnerabilities in systems and networks of all kinds. One of the early well known UNIX scanners, SATAN (System Administrator Tool for Analyzing Networks), later morphed into SAINT (Security Administrator’s Integrated Network Tool). These names illustrate the disparate dual nature of the purposes to which such tools can be put.

In the hands of a would-be intruder, vulnerability scanners become a means of finding victims and determining those victims’ weak points, like an undercover intelligence operative who infiltrates the opposition’s supposedly secure location and gathers information that can be used to launch a full scale attack. However, in the hands of those who are charged with protecting their networks, these scanners are a vital proactive defense mechanism that allows you to see your systems through the eyes of the enemy and take steps to lock the doors, board up the windows, and plug up seldom-used passageways through which the “bad guys” could enter, before they get a chance.

In fact, the first scanners were designed as hacking tools, but this is a case in which the bad guys’ weapons have been appropriated and used to defend against them. By “fighting fire
with fire,” administrators gain a much-needed advantage. For the first time, they are able to battle intruders proactively.

**Proactive vs. reactive security**

There are two basic methods of dealing with security breaches:

- The reactive method is passive; when a breach occurs, you respond to it, doing damage control at the same time you track down how the intruder or attacker got in and cut off that means of access so it won’t happen again.
- The proactive method is active; instead of waiting for the hackers to show you where you’re vulnerable, you put on your own hacker hat – in relation to your own network – and set out to find the vulnerabilities yourself, before anyone else discovers and exploits them.

The best security strategy employs both reactive and proactive mechanisms. Intrusion Detection Systems (IDS), for example, are reactive in that they detect suspicious network activity so that you can respond to it appropriately.

Vulnerability assessment scanning is a proactive tool that gives you the power to anticipate vulnerabilities and keep out attackers, instead of spending much more time and money responding to attack after attack. The goal of proactive security is to prevent attacks before they happen, thus decreasing the load on reactive mechanisms. Being proactive is more cost effective and usually easier; the difference can be illustrated by contrasting the time and cost required to clean up after vandals break into your home or office with the effort and money required to simply install better locks that will keep them out.

Despite the initial outlay for the vulnerability assessment scanners and the time spent administering it, potential return on investment is very high, in the form of time and money saved when attacks are prevented (see *Consequences of Security Breaches* below).

**Vulnerability Assessment Scanning Hacks Your Network – Before a Hacker Does**

The number of security breaches – and attempted breaches – has steadily increased over the years. Even as operating system vendors and applications vendors scramble to patch the holes in their products, tech-savvy intruders uncover new exploitable flaws. In today’s environment, where persistent connectivity is a business necessity and accessibility of resources can make the difference between business success or failure, no piece of complex software can be 100% secure out of the box.

A modern operating system is made up of millions of lines of code, and that kind of complexity makes it virtually impossible for developers – regardless of how vigilant they may be – to find all potential vulnerabilities before the software goes into production use. Add to this the many applications that run on top of the operating systems, created by different companies, and the lack of absolute standards within the industry, and the inevitability of vulnerabilities becomes apparent.
It would be difficult, time consuming and prone to error to manually check the settings and patch status of every network device and computer on your network. In an enterprise environment, it’s not just difficult; it’s impossible. Another way to discover vulnerabilities is via manual penetration testing, but again, the task is overwhelming on all but the smallest networks. With vulnerability scanners, you can automate the process, making it fast and simple regardless of the size of your network. These scanners can probe your network devices and systems for weak spots, and some scanners will emulate real-world attacks and analyze the results.

Nonetheless, surveys show that many organizations don’t use security scanners. According to Sunbelt Software’s Security Vulnerability Scanner Survey, 55% of respondents use vulnerability scanning as part of their network security strategy. A similar survey conducted by InfoWeek Magazine found that out of more than 2500 responding companies, only 23% use vulnerability assessment tools. These findings indicate that there are a large number of networks that are not taking advantage of the benefits of scanning as a preventative tool.

**Importance of Vulnerability Assessment to Network Security**

When a vulnerable system is connected to the Internet on a 24/7 basis, you can be assured there will be intruders “knocking on the door” sooner or later – probably sooner. And if those vulnerabilities aren’t addressed, they’ll get in. The Internet Software Consortium reported in January 2003 that there were almost 200 million hosts found on the Internet. (is there more recent data?) In any community that large, there are sure to be some who are looking to take advantage of the unprotected. Modern hacking tools, available to anyone free of charge, make it easier than ever for attackers to ferret out and exploit existing security holes, and do it with a high degree of anonymity. Motives vary from “just for fun” to personal vendettas or monetary gain, but regardless of their reasons, there are hordes of hackers out there, either targeting specific networks or randomly “cruising” for victims.

Just as a car thief is always keeping an eye out for unlocked vehicles, network intruders are always on the lookout for misconfigured, unpatched and unprotected systems that they can “grab” quickly and easily. When you park your car on the street in a high crime area, you check to ensure that the keys are out, that all doors are locked, that no valuables are in sight, perhaps even use a steering wheel lock or other anti-theft device for extra protection. It’s just as important to regularly check the security status of your network (more so, considering the potential loss in money, time, productivity and even the organization’s reputation if a serious breach occurs).

In May 2003 in its eighth annual Computer Crime and Security Survey (free copy available at http://www.gocsi.com/forms/fbi/pdf.jhtml), the Computer Security Institute (CSI) in conjunction with the FBI reported that 92 percent of the respondents had been attacked, with overall financial losses of over $200 million reported by 251 of the organizations. 75 percent of the respondents acknowledged that they had suffered some financial loss due to attacks.
How Vulnerability Assessment Fits into your Multi-Layered Security Plan

A good network security plan is multi-layered, just like a good physical security plan. In defending your home or business against intruders, you don’t rely on just one security mechanism. Instead, you have fencing (and perhaps a big dog) to guard the perimeter, strong locks on the doors to control access, an alarm system to alert you of unauthorized entry, and perhaps a safe to protect special valuables. Likewise, no single technology or software program can provide complete protection for your network. You need perimeter security (firewall), access controls (permissions), alerting mechanisms (intrusion detection) and perhaps encryption to protect particularly sensitive files.

Just as you perform maintenance on your alarm system and install newer, better locks when they become available, you must constantly assess your network security mechanisms. Security is an on-going process. Vulnerability assessment is an important element because it tests the effectiveness of your other security implementations. You might feel safe because you’ve applied X number of patches or followed recommendations to shut down specific services. But remember that many popular exploits don’t rely on obscure, unused services and protocols that you can easily disable without affecting network usability. Instead, they use HTTP, FTP, SMTP and other protocols that are vital to your users’ ability to communicate and do their jobs. Attacks such as Code Red and Nimda had such a devastating effect because they exploited flaws in mission critical software such as IIS, Outlook and Internet Explorer.

Are there still security holes lurking in your system? Only a concerted effort to get inside your network can tell you that. It’s far better if that effort comes from software vulnerability assessment scanner controlled by you, rather than from the actions of an intruder.

How a Comprehensive Security Plan Gives Your Company a Competitive Edge

Does your organization do any of the following?

- Sell products or services via e-commerce
- Do business with your customers, partners and vendors via e-mail
- Depend on your web site to get your advertising message out and/or provide product support
- Share information within the company via an intranet
- Make data available to employees or the public through an FTP server
- Use the Internet to conduct research, verify information, or establish contacts

If so, a serious security breach can not only cost you money, time, sales, and goodwill; it can give your competitors an advantage. Likewise, preventing attacks before they happen gives your company a competitive edge. While your competitor is busy scrambling to recover from the next big exploit, you’ll be conducting business as usual (and maybe better than usual, when your competitor’s frustrated customers come to you instead).

In today’s highly competitive business environment, market share can be like a horserace; once you get behind, it’s difficult to catch up. Even a few days – or in some cases, a few hours – of network downtime can put a company hopelessly behind the competition. A
comprehensive, well-planned security strategy that includes proactive vulnerability assessment scanning can keep you ahead of the pack.

There is no such thing as 100% security, but intelligent risk management strategies (such as taking preventative actions against attackers) increase the chances that you won’t lose competitive ground when the next wave of exploits comes.

Vulnerability Assessment Technologies: How They Work

Deciding to implement a vulnerability assessment program is an important first step in keeping your systems safe from intruders. The next, equally critical step is selection of the right technology to fit your organization’s needs. All vulnerability scanners are not created equal, nor do they cost the same. It’s important to weigh a number of factors, including:

- Underlying technology (for example, passive vs. active scanning, host vs. network scanning)
- Features
- Number of vulnerabilities in the database
- Ease of use
- Reporting features (comprehensiveness, configurability and customization, format, methods of output)
- Analysis and recommendations for remedial action (does the software only report what’s wrong, or does it tell you how to fix it?)
- Accuracy of analysis (prevalence of false positives/negatives)
- Security issues (does the scanner itself pose a security risk, as with some scanners that not only expose vulnerabilities but automatically exploit them?)
- Performance
- Pricing structure

Underlying Technology

The first thing to look at in comparing vulnerability assessment scanners is the underlying technology. You’ll want to compare passive vs. active scanning, host vs. network scanning, and so forth. Some scanning solutions are Internet-based, with the management and aggregation server residing on the vendor’s system, rather than the customer’s site. The advantage of this is that attack signatures are always up to date. The disadvantage is that your organization is dependent on the vendor’s server to perform the scans.

Scanning solutions range from simple “port scanners” that probe for open ports to scanners that check for security patches, scans the registry, verifies compliance with security policies, or emulates full fledged attacks on your systems.

The scanning process itself can be classified as “passive” or “active.” Passive scanning is designed not to generate network traffic that can crash the target systems. Passive scanners analyze normal network traffic and can be implemented as “always on.” They work more like a network monitor or IDS than an active scanner.
Active scanners are more “aggressive” and can interfere with the operation of the network and target systems. They do not run continuously; instead a scan is performed at regular intervals.

Host-based scanners require that agent software be installed on each host, while network-based scanners do not. A network-based scanner may require a dedicated computer to run the scanning solution, because it uses a significant amount of resources. For a good discussion of network vs host-based scanning, see Vulnerability Assessment: Network Based versus Host Based, at http://www.giac.org/practical/GSEC/Robby_Fussell_GSEC.pdf.

You’ll also want to look at whether the scanner is capable of scanning different systems (e.g., Microsoft, UNIX, NetWare) if you have a multi-vendor environment.

**Features Administrators Want**

In general, vulnerability scanners perform the following functions: scanning/mapping, reporting, analysis and recommendations, and data management. In many respects, scanning is the easy part. Management of the information and accurate analysis of scan results is equally important. Another feature to consider is notification; does the scanner alert administrators when vulnerabilities are found? What is the method of notification?

Features administrators most often mention wanting in a software vulnerability scanner include:

- Good reporting capabilities
- Ease of installation and use
- Detection of missing patches
- Fast performance and the ability to fix vulnerabilities quickly
- Dependable detection of vulnerabilities and vulnerability ranking
- Scalability
- Easy updating
- A cost-friendly pricing structure

**Vulnerabilities database**

Before a scanner can detect a vulnerability, that vulnerability must be in its database, so the number of entries in the vulnerability database determines how comprehensive the scan will be.

However, numbers don’t tell the whole story. The real test is whether the scanner catches the most common vulnerabilities, and ultimately, whether it detects the ones that affect your systems. An inventory of your network assets will determine the types of network devices and systems you have; you’ll want to use a scanner with a database that checks vulnerabilities specific to your environment. For example, if you have many NetWare servers, a scanner that doesn’t include NetWare vulnerabilities isn’t the best choice.
Of course, attack signatures within the vulnerabilities database must be updated frequently in order to detect newly discovered security flaws.

**Ease of Use**

An interface that is difficult to understand and use will discourage administrators from using the tool, so user-friendliness is an important consideration. Interfaces range from simple text-based to complex graphical interfaces to web interfaces.

**Reporting**

Reporting capability is of growing importance to administrators, in a documentation-oriented business climate where you must not only be able to do your job, but also provide written proof of how you’ve done it. In fact, respondents to Sunbelt’s survey indicate that flexible and prioritizing reporting is their number one favorite feature.

A scan might return hundreds or thousands of results, but the data is useless unless it is organized in a way that it can be understood. That means that ideally you will be able to sort and cross-reference the data, export it to other programs and formats (such as CSV, HTML, XML, MHT, MDB, Excel, Word, and/or Lotus), view it in different ways, and easily compare it to the results of earlier scans.

Comprehensive, flexible and customizable reporting is used within your department to provide a guideline of technical steps you need to take, but that’s not all. Good reports also give you the ammunition you need to justify the costs of implementing security measures to management.

**Analysis and Recommendations**

Finding out what the vulnerabilities are is only half the battle. A complete solution also tells you what to do about them. A good vulnerability scanner analyzes the scan results and provides recommendations for remedial action. Some scanners do this within the report; others provide links to the vendor’s web site or other online resources.

Vulnerability remediation tools also exist, which work in conjunction with popular scanners to aggregate the results of the scans and automate the remediation process.

**Accuracy of analysis**

A comprehensive report with detailed recommendations for remedial action is great, but only if the reported results are accurate and the recommended actions are effective. A good scanner must have a low rate of false positives (in which vulnerabilities are reported that do not in fact exist) and false negatives (in which vulnerabilities that do exist are not detected).
Security Issues
A scanner that brings down the network can result in many of the same financial losses as a real attack. Some scanners are capable of going a step further than just finding exploits and can actually attempt to use them. This is a great way to ensure that the vulnerability is real and eliminate the possibility of a false positive, but unless it is expected and planned for, it can cause the very problems it’s supposed to prevent. Scanners that have this capability should be used with great care, and should be configured so that exploits don’t occur automatically.

Another way the scanner itself can disable your network is by creating a denial of service (DoS) due to the traffic overload from the scanning process. It’s important that the scanner’s assessment settings be fine tuned to prevent this. The ability to configure such items as number of concurrent running threads, packet interval and total number of scan objects lets you make adjustments to minimize the impact on the network. Some vulnerability assessment scanners provide a “safe scan” template designed to prevent outages to target systems.

Performance
A vulnerability scanner can use a lot of network bandwidth, so you want the scanning process to complete as quickly as possible. Of course, the more vulnerabilities in the database, and the more comprehensive the scan, the longer it will take, so this can be a trade-off. One way to increase performance is through the use of multiple scanners on the enterprise network, which can report back to one system that aggregates the results.

Vulnerability Assessment Scanner Pricing Structures
Vulnerability assessment scanners range in cost from free to thousands of dollars. Following the old adage that “you get what you pay for,” freeware scanners tend to be simpler and less scalable, sport fewer features, skimp on important features such as reporting, and/or require mastery of a less user-friendly (often character based) interface.

Commercial scanning products can be licensed in one of several ways: per IP block, per server, or per administrator. The licensing structure can have a significant impact on how much your organization ends up paying for a vulnerability scanner.

Per IP Block
Several popular products, such as eEye’s Retina and Internet Security Scanner (ISS) require that enterprise customers pay per IP block or range. In other words, pricing depends on the number of IP addresses to be scanned. Licenses are purchased via an “IP pack,” consisting of a set number of IPs (for example, 16, 32, 64, 128 or 256). Generally, the pack allows you to scan a range of IPs up to the number indicated on the license pack.

One problem with this is that if you have 65 IPs to be scanned, you may be required to buy a 128 IP pack. For one popular product, a 64 IP pack costs $2550, while a 128 IP pack costs $4080. Thus you will have to pay over $1500 for that single, 65th IP. Some vendors may
allow you to purchase individual IP licenses, but it is the consensus of respondents to the Sunbelt Software survey that per-IP is the least popular licensing scheme. Consequently, only 11 percent of respondents were paying per IP block.

Per-IP licensing may also become complicated when you have a number of multi-homed systems, either computers with multiple addresses bound to a single interface or computers with more than one network interface and thus multiple IP addresses assigned to one machine.

**Per Server**
Some vulnerability scanner vendors charge a per-server and/or per-workstation licensing fee. This fee can be much higher for servers than for workstations, significantly increasing the cost of licensing if there are multiple servers involved.

**Per Administrator**
Sunbelt’s survey showed that well over 50 percent of respondents prefer a per-administrator (or per-seat) pricing structure for a security scanner. This licensing scheme is simpler and more cost effective for most organizations.

**Who’s Using Vulnerability Assessment and What Are They Using?**
There are dozens of vulnerability assessment utilities available, ranging from the free Microsoft Baseline Security Analyzer (MBSA) to a variety of commercial products. Sunbelt’s survey showed that, of the 55 percent of respondents who use a security scanner, the largest number use the MBSA (20 percent), followed by Nessus, another free program (17 percent). Complete results for this question are shown in Table 1.

<table>
<thead>
<tr>
<th>Vulnerability Assessment Scanner</th>
<th>Percentage Using It</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Baseline Security Analyzer</td>
<td>20%</td>
</tr>
<tr>
<td>Nessus</td>
<td>17%</td>
</tr>
<tr>
<td>LanGuard (GFI)</td>
<td>14%</td>
</tr>
<tr>
<td>Retina (eEye)</td>
<td>13%</td>
</tr>
<tr>
<td>Internet Security Scanner (ISS)</td>
<td>11%</td>
</tr>
<tr>
<td>Nmap</td>
<td>6%</td>
</tr>
</tbody>
</table>

80 percent of those who use vulnerability scanners say they like their current scanning solution. 20 percent described the scanner as “invaluable” in protecting their networks.

**Who’s Not Using Vulnerability Assessment Scanners — and Why**
If vulnerability assessment tool users are so happy with the scanners, why do 45 to 77 percent of administrators (depending on the survey) not use vulnerability assessment technology to protect their networks? The reasons given most often come down to the “usual suspects”: time and money – along with some “human factors.”
Cost factors
The high cost of many of the commercial scanner products (along with complicated licensing schemes that make it difficult to determine just what the bottom line cost will be) is a deterrent when it comes to implementing another new security measure such as vulnerability assessment. Although these commercial solutions may be more fully automated and offer a softer learning curve than their freeware counterparts, many IT departments are operating on much tighter budgets than they were in the 90s, so cost counts.

Time factors
If money is the problem, why not use one of several available freeware solutions? At a point in time when economic problems throughout the tech sector and other industries, along with resultant budget cutbacks, have IT departments understaffed and overworked, the perceived time and effort required to conduct vulnerability assessments is a major factor. Many network administrators would like to add vulnerability assessment tools to their security plans, but simply don’t have the time to implement a complex new product, especially one that’s not particularly user friendly.

The “It Won’t Happen to Us” Factor
Practical matters aside, CEOs, CIOs and administrators are all human beings and thus subject to normal human tendencies – including the tendency to assume that bad things happen to “other people,” not to us. Organizational decision makers assume that their companies aren’t likely targets for hackers (“Why would an attacker want to break into the network of Widgets, Inc. when they could go after the Department of Defense or Microsoft or someone else who’s much more interesting?”).

But remember that more than 90 percent of the businesses in CSI’s survey reported that they’d been attacked. This indicates that the chances of an attack are high for all companies. Even if your network isn’t directly targeted, many of the most harmful threats come from worms and other malicious code that is sent randomly.

Consequences of Security Breaches
The CERT Coordination Center received over 114,000 vulnerability incidents reported in the first through third quarters of 2003 (significantly more than reported for all of 2002). This indicates that such incidents are increasing, which means the odds that your organization will be victimized are increasing, as well.

What does a security breach really mean to your company? That depends. Depending on the particular exploit, the motivations of the attacker, what data you have on the network, and the role the network plays in your business, results of a breach can range from mere inconvenience to the loss of millions of dollars.
Direct financial loss
According to the CSI report, the greatest monetary losses reported by companies were due to theft of proprietary information. Most organizations have data stored on their networks that is confidential and crucial to how they make their products or provide their services.

Cost of downtime in productivity
CSI survey respondents reported that the second greatest losses were due to denial of service (DoS) attacks. The lost productivity and lost sales during network “downtime” can add up to thousands or even millions of dollars.

Lost future business: the “ripple effect”
A less obvious ramification when network connectivity is lost is the loss of confidence from customers and partners. This can have a financial impact extending far beyond the actual time period during which the network is out of use.

Litigation/legal factors
Many industries and fields today fall under government regulations that require compliance with specific rules regarding the protection of digital information. Examples of such regulations include:

- The Health Insurance Portability and Accountability Act (HIPAA), regulating health care providers
- The Gramm-Leach-Bliley Act (GLBA), regulating financial services
- NASD/SEC rules, regulating the securities industry
- Sarbanes-Oxley Act of 2002, regulating public company accounting

Failure to comply with the requirements of these federal laws (as well as a diversity of state regulations) by allowing protected information to become available to unauthorized persons through security breaches can subject companies to fines, civil litigation and other legal penalties, even criminal charges.

Why SNSI is the Best Choice for your Vulnerability Assessment Needs
Because so many companies report that lack of time and high cost are the two factors preventing them from using a vulnerability scanner, SNSI focuses on making it quick and easy to install and use the product, as well as keeping costs low – while still providing you – the administrator - with the benefits of a fully developed commercial-grade scanner.

How SNSI Addresses the Problems That Prevent Companies from Using Vulnerability Scanners
SNSI features “five click” installation, taking the dread out of deploying typical scanner solutions. But ease of use doesn’t end with installation. The “fast config” feature means it won’t take you days of reading help files, calling tech support and resorting to trial and error to get your scanner set up and ready to start detecting vulnerabilities on your network. The
simple “point and click” graphical interface lets you scan and analyze a single computer or an entire domain, and you can set up custom “quick scans” to only select specific vulnerabilities and ignore others.

You get instant scan results, in an understandable and usable format, so that you don’t have to spend hours waiting for the scans to complete and then more hours trying to decipher what your scanner found.

How SNSI Prevents the Consequences of Security Breaches
A vulnerability scanner is only as good as its database, and SNSI boasts the best: a top-rated “milspec” vulnerability database (military specification quality). The database contains over 2,500 unique known security vulnerabilities and is updated regularly so you won’t fall prey to newly discovered vulnerabilities.

In addition to a comprehensive database of ranked vulnerabilities, SNSI provides excellent, organized reports so all its results are completely documented. Reports can be easily customized for the audience (IT administrator or executive management).

You’re not left in the dark with a list of detected vulnerabilities and no idea what to do about them; SNSI gives you easy to follow instructions for plugging the critical holes to prevent exploits now. SNSI uses the latest Mitre Common Vulnerabilities and Exposures (CVE) list of computer vulnerabilities and contains the latest SANS/FBI top 20 vulnerability list. It also uses the latest CERT, CIAC and FedCIRC (Department of Homeland Security) advisories. You’ll get detailed analyses of the name, description and risk level of each vulnerability, along with references and Knowledge Base links describing how to eliminate them. You can also retest the corrected vulnerabilities to ensure that the security holes have really been patched.

How SNSI Pricing Structure Saves your Company Money
The SNSI pricing structure is designed to save your company money and simplify the licensing process. In keeping with the wishes expressed by IT pros who work in the real world, SNSI licenses are sold on a per-administrator basis, with no limits on the number of machines – a welcome change for those who have been paying for scanning licenses per IP range.

Because time is money, now more than ever, SNSI also indirectly decreases your TCO, by keeping your network up and running, and by freeing your IT personnel to juggle their already heavy workloads without worrying about “babysitting” the vulnerability scanner. SNSI won’t make a hole in your budget while it finds the holes in your network.

Summary
In today’s interconnected network environment, threats can come from anywhere. An attacker half way around the world can find and exploit your network vulnerabilities as easily
as can someone down the block. The first step in defending yourself is knowing where the holes are – and plugging them – before an intruder uncovers them and uses them against you. The easiest way to do that is by utilizing a vulnerability assessment scanner.

But vulnerability scanners differ widely in features, accuracy, cost and usability. Freeware may save you money upfront but cost thousands (or millions) of dollars in administrative time due to the failure of the scanner to detect and address critical flaws. The best vulnerability assessment tool for your network is the product that gives you the best return on your investment. That means a product that’s quick and easy to install and use, with reporting capabilities that document results in a flexible and easy to understand format, with a comprehensive database of known vulnerabilities, and with a fair, simple and cost-effective licensing structure. Sunbelt’s SNSI was specifically designed to meet all these requirements, so your company can get on with the business of doing business.

REFERENCES


