



PREDATORWATCH

**How a Simplified Turnkey Vulnerability Management System Can
Help You Achieve Proactive Network Security**

Achieving True Proactive Network Security

by Gary S. Miliefsky, CISSP®

**For more information, visit us online at:
www.predatorwatch.com**

*Copyright © 2003-2005, PredatorWatch, Inc.
All right reserved worldwide.
PredatorWatch Auditor products are CVE-Compliant.*

Achieving True Proactive Network Security

With hackers hard at work, only the right equipment can you really keep hackers off your company's network.

You Are Being Hacked

Hackers are working harder than ever—attempting to gain access to your network. Hacking has been a problem for years. Known threats have been tracked, but even as solutions to combat those threats have evolved, the number of network intrusions from hackers has grown from 1,000 in 1990 (not trivial) to over 137,500 in 2003 (source: CERT).

Hackers Impact Productivity, Destroy Data

Hackers interfere with productivity—they generate denial of service (DoS) attacks, change the root password to lock out your key personnel while letting themselves in. They stop vital services, crash the server, bring the entire network down.

Hackers destroy data. They sneak in the back door by defeating protocols that use date and time of day, crashing machines where vital work is in process, and causing data loss. Other ways that hackers destroy data include overwriting “good” data with garbage data, executing PHP code on a system, or executing system administrator commands to erase data, alter access, and create havoc.

Hackers Put You at Risk

Malicious intruders can steal private data, even identities. By getting into private accounts, accessing or pilfering private data, they can put you at risk for legal liability or non-compliance with regulatory requirements such as Sarbanes-Oxley (accounting),

HIPAA (health care), GLBA (financial), FDA requirements,

Between denial of service, and destruction and theft of data, hackers can damage your company.

Countermeasures Alone Are Not Enough...

Even with the gamut of protections from anti-virus to a solid firewall, your network is still be open to hacking. While virtual private networks (VPNs), spam protection, local browser JavaScript protection, and email passwords serve vital functions, hackers can defeat them all.

Of course, you should have information security (INFOSEC) equipment such as routers and firewalls. .And you

Hackers are taking advantage of Common Vulnerabilities and Exposures (CVEs).

You can stop hackers by finding & eliminating these weaknesses in your network.

must employ encryption servers such as Internet Protocol security (IPSEC) and secure socket layer and/or transport security layer (SSL/TLS).

And of course deploying hypertext transfer protocol secured (HTTPS) is required, along with public key infrastructure (PKI) to encrypt data. Even having a content proxy for filtering access and accelerating the Internet are wise. Still your network is not adequately protected.

Another level of protection that is becoming vital is having an Intrusion Detection System (IDS). But these systems find intruders only after they have already broken in. It makes more sense to secure the doors, so hackers never cross the threshold.

New Technology Means New Risks

And what about the newest technologies? Wireless connection points that a roving war driver can use to get onto your network open doors that previously never existed. An employee can plug in a wireless device and open a vulnerability right there. PDAs may have vulnerabilities that a hacker could tap into. What about laptops? Because they roam outside the organization, plugging in to other networks, they are often home to vulnerabilities. But you cannot restrict employees (66% of the workforce will be mobile by 2006, SOURCE: International Data Corp). Instead you need to monitor mobile devices when they plug in and block them *if they contain vulnerabilities*.

As Long As There Are Hackers Out There...

As long as there are hackers out there, you can't be sure data assets are protected. Your intellectual property is at risk. You can't be sure you're in compliance with regulations. You can't be sure you're avoiding legal liability. Is there a solution to this problem?

What Can You Do?

Well, take a look at your options. You could go back to using paper and turn off access to the Internet—not a solution. You'd lose productivity and ultimately lose in terms of return on

investment (ROI) and total cost of ownership (TCO). The Internet has been a great growth tool, a great information resource. Your business depends on the Internet to obtain clients and receive email communications. Cutting off access to the Internet is not a solution. Instead, you need to secure your network, to be sure it is not vulnerable to attack just because you are on the Internet.

Comprehensive Approach

What you really need is a comprehensive approach to corporate security. For your buildings, you have security guards. You do a background check, bond them, properly train them, supply them with metal detectors and scanners.

A vulnerability management system is similar. The network needs guards. Eighty percent of attacks are perpetrated by insiders, whether malicious or not. After a downsize, some personnel may still be able to get past past the INFOSEC equipment you have in place. You need a system that can stop possible intruders at every entryway.

You Need a Corporate Security Policy

A modern corporate security plan and policy must encompass both a virtual perimeter of protection around the network and a regular audit process. An audit system must check the entire network at particular intervals. You require a proactive system that is reliable and self-managing.

You Need Proactive Solutions, Not Reactive

If you are using a firewall and IDS, you are still deploying reactive solutions. By the time you find out about the problems, the hackers have already done the damage.

Hackers take advantage of common vulnerabilities in your network. What you need to do is audit constantly to determine what your network's vulnerabilities are and then make changes as required to prevent hackers from exploiting them.

This proactive approach is the only reliable way to protect your network.

Auditor Proactively Helps Stop Threats

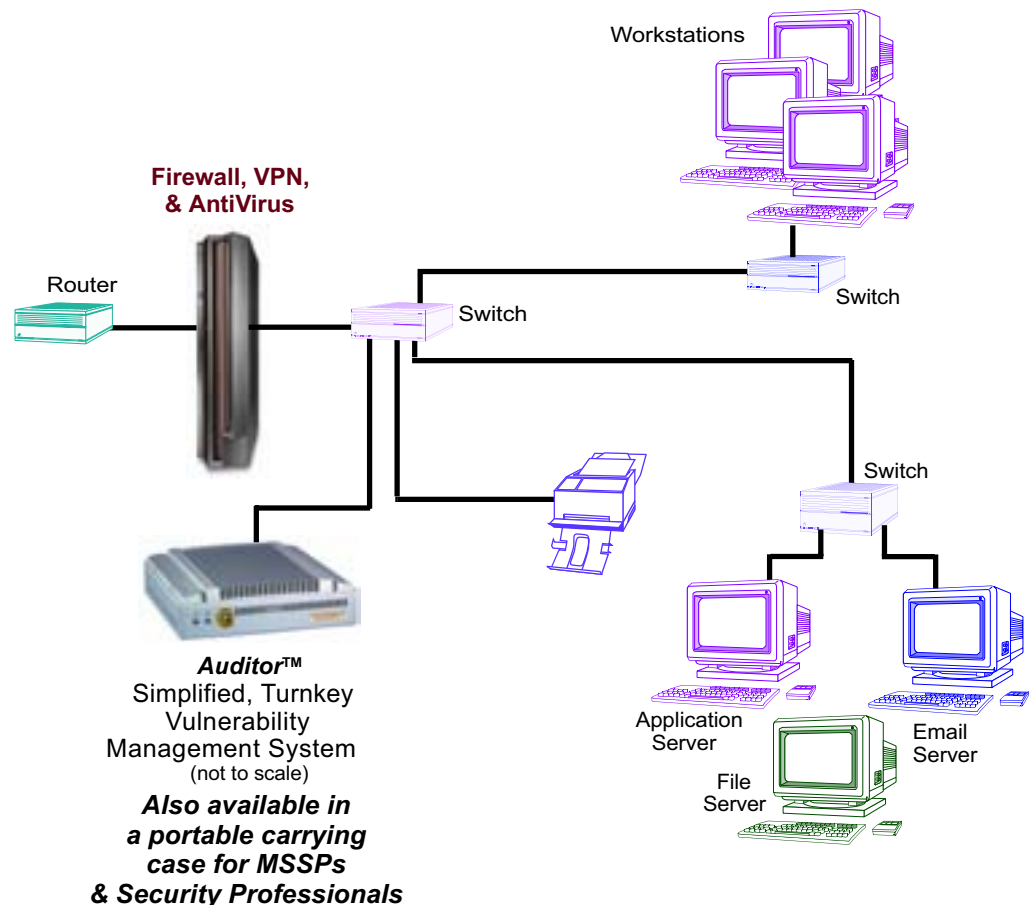
An aggressively proactive network security solution is the **Auditor** vulnerability management system. **Auditor** provides a tamperproof solution that stops intruders by helping you plug all the holes in your network. It audits your network regularly and consistently against the Common Vulnerabilities and Exposures (CVEs) database maintained by the MITRE Corporation. It regularly updates itself with knowledge of the latest known vulnerabilities. It goes further than mere vulnerability assessment, however, because it is constantly monitoring your network and detects rogue devices on plug-in. It integrates with your countermeasures, strengthening them. Let's take a look at how it works.

How Auditor Works

You install the **Auditor** vulnerability management system on your network. It is in a small appliance that you configure once, then set to work.

You plug it in to the first switch inside your firewall and let it scan for systems present. It picks up their IP addresses and you select which nodes you want audited and how often.

Each time **Auditor** audits your network, it identifies all actual and potential security holes. You start by defining multiple audit profiles, maybe one for each subnet, and one for each



critical server, such as an email server, financial database server, or file server.

You schedule the audits daily, weekly, or monthly. You tell **Auditor** who in your organization should receive reports on the results of these audits—the system administrator or a key manager. You can have the most detailed report go to a system administrator and the executive report go to the CEO.

You then set the schedules in motion. That's it. From then on, **Auditor** does the work, constantly and vigilantly, without teams of expensive personnel to oversee it.

When a system administrator receives an **Auditor** report, that report includes straightforward instructions on how to proceed to resolve vulnerabilities. The first reports are baseline reports from **Auditor**. Subsequent reports can be restricted to finding still remaining vulnerabilities and/or new vulnerabilities discovered.

Keeping up with **Auditor** reports is a small task compared to work required in a reactive situation. No more running around, shutting down systems. No more races against the intrusion's affects. Proactive prevention reduces the chaos, puts you in control.

Auditor Updates Itself

Auditor works by testing your network for the Common Vulnerabilities and Exposure (CVEs). As new CVEs become known, it regularly updates itself with the latest known vulnerabilities through a secure port in your firewall.

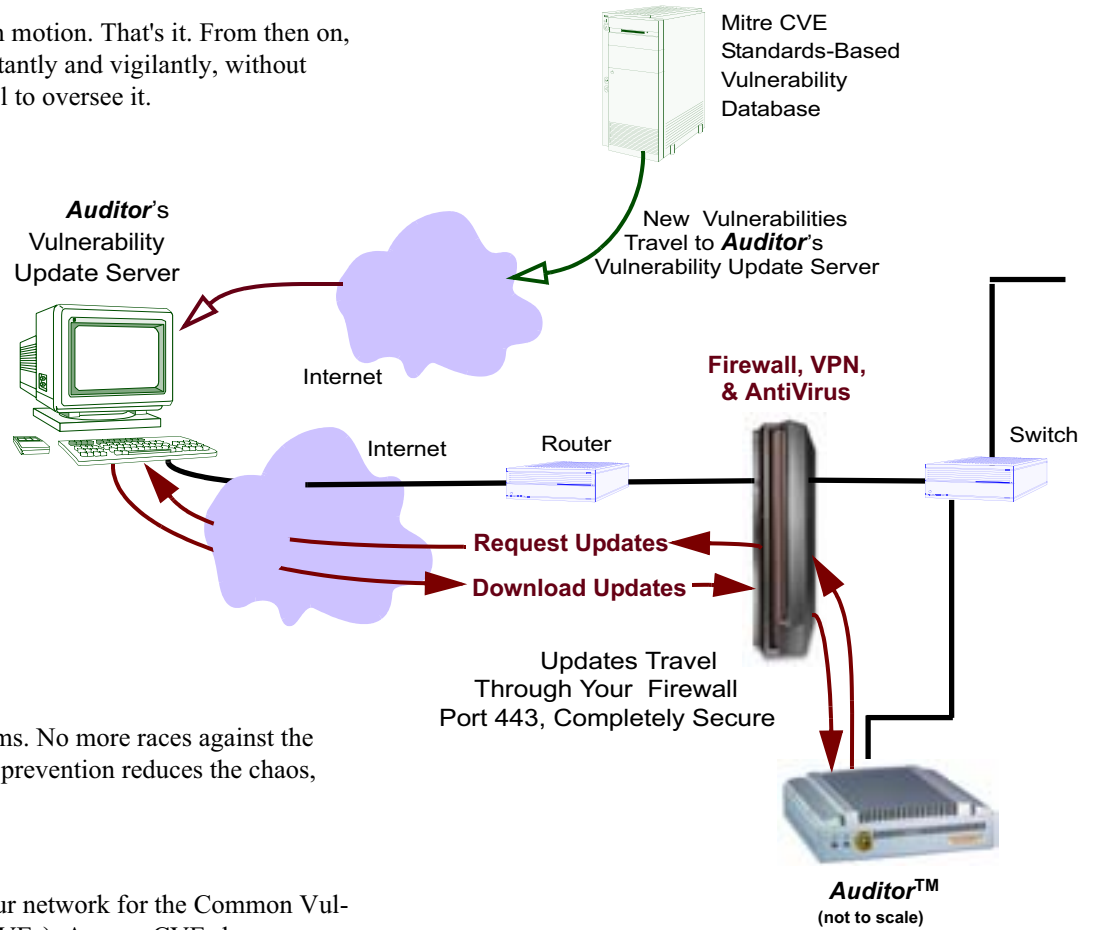
It retrieves those updates from the **Auditor** Vulnerability Update Server, which works with standards-based vulnerabilities, the CVE standard, maintained by MITRE Corporation and backed by the US government.

Dynamic Detection of Laptops and Rogue Wireless Connection Points

A unique feature of **Auditor** is its ability to instantaneously detect systems that plug in to your network. It detects laptops, rogue wireless connection points, wireless devices, and other mobile equipment—even PDAs—that have just plugged in, and immediately sends an alert to the IT manager via email and/or cell phone. By constantly monitoring for and detecting new and mobile devices on the network, **Auditor** maintains a vigilance level above that of every competitor.

FirewallBooster with Clientless Quarantine

Not only does **Auditor** dynamically detect devices on connection, it also immediately audits them once they are on the network. If a vulnerability exists on any of these dynamically detected devices, **Auditor**'s FirewallBooster works in concert with your firewall to block traffic to and from vul-



nerable ports—helping deliver on the full potential of your firewall.

Plus it sends vulnerability alerts to the IT manager through both email and cell phone, keeping IT constantly informed of the network status.

And you don't have to install client software on the network's machines, because the FirewallBooster effectively performs a **Clientless Quarantine** on the vulnerable system—keeping it quarantined until it is cleared of vulnerabilities. It can perform this clientless quarantine on any system, whether or not it has been previously known, whether it is trusted or untrusted.

Special options let you tell **Auditor** to tailor its request to the firewall, having it block access to ports only or to the entire

IP address. You can also set up a *safe list* that indicates to **Auditor** those systems that should never be blocked.

Auditor Helps You Manage Your Assets

Alongside its unique dynamic detection/FirewallBooster/Clientless Quarantine system, **Auditor** also has a network monitor that constantly checks to be sure assets are responsive. It sends InventoryAlerts when systems are missing or in trouble.

Its AssetTracker allows you to associate information about software, users, and peripherals with each system, helping you maintain the network while protecting it.

Auditor Performs Non-Intrusive Audits

Unlike an IDS, **Auditor** is not in the critical path and never interferes with normal network activity. You can set it to function on low bandwidth or utilize the option of increasing audit speed by using greater bandwidth when permissible. Such flexible options help you achieve on demand results, but never compromise system efficiency.

With flexible options, **Auditor** lets you both schedule audits to occur automatically and execute audits on demand.

Targeted Reports

Auditor reports are targeted to executives, managers, and system administrators. Executive and manager reports help plan and strategize, while system administrator reports help pursue vulnerability remediation. **Auditor** reports also provide an audit trail for regulatory compliance.



To help you keep records, **Auditor** stores from 60 MB of audit profiles/reports (smallest model) to upwards of 10 GB (rack model). **Auditor** comes in three major models, **Auditor 16** (or **Laptop Auditor**) for branch offices or single subnets with up to 16 IP addresses, **Auditor 128** for small-to-medium enterprises with up to 254 IP addresses, and the **Auditor Enterprise** for larger networks with over 255 IP addresses.

For MSSPs and other security professionals, **Auditor** is available in a portable carrying case for transport from site to site.

Auditor Is Easy to Use

The **Auditor** vulnerability management system does not require teams of high-level personnel to interpret its results; instead, it sends easy-to-understand reports on vulnerabilities and straightforward remedies to resolve them.

With Auditor You Reap a Quick ROI

And you'll obtain a quick return on your investment (ROI) with **Auditor**, because the product readily pays for itself, even in small-to-medium enterprises.

As it protects your network, it saves untold hours of downtime and of reworking corrupted/lost data. It protects you from legal liability and regulatory compliance issues.

Auditor Is Operating System Independent

The **Auditor** probes any network for hackers, regardless of what operating system or systems you may be running. It works with Linux, all flavors of Windows, Cisco IOS, all types of UNIX, VXworks, and many more.

Why an Appliance?

Since **Auditor** is housed in an appliance, you don't have to buy a dedicated computer (as you would for a software product) and harden it to ensure it can't be hacked, then install software on it. **Auditor** does all of that for you.

In fact, the **Auditor** appliance is tamperproof. No one can hack in and generate a denial of service (DoS) to the appliance. It has rigorous password protection and secure socket layer (SSL). The system's hardened OS has special programs that make its files read-only so that no one can hack them. Plus it has Tripwire logging events and sending alerts when a break-in attempt occurs. **Auditor** monitors itself, checking for high availability of its own programs.

You Own the Data

All data collected by the **Auditor** remains the property of the customer. You own all reports. PredatorWatch adheres to strict enterprise security guidelines that require critical data to remain within *your* trusted environment, never posting your data to any web site, "secure" or otherwise.

Summary

Being proactive means building a solid foundation so your network performs and your people can do their work, minimize downtime, and focus on core competencies—instead of reacting to an attack on a known vulnerability after the fact. **Auditor** can help institute proactive network security.

The Auditor Challenge

Call PredatorWatch (978) 251-0823 or (866) 667-4462. We can stop by with a demonstration unit and show you in less than 1/2 hour how vulnerable your network may be to insider threats and attacks by hackers. Visit PredatorWatch at: www.predatorwatch.com.