



Certified to find:



Auditor XL - World's Smallest Auditor

"Audits network against one or more specific regulatory requirements; quarantines vulnerable systems until security holes are fixed."

SmallBusinessComputing.com - 02/05

The Problem with Network Security Today

The four key pillars of network security: Anti-virus, Firewall/VPN, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) do not protect your network assets from hackers, viruses, worms and spyware nor help you to comply with government regulations. In addition, none of these solutions have been able to properly alert, block and remediate against dirty laptops, untrusted and malicious insiders as well as rogue wireless devices.

In summary:

1. INTERNAL VULNERABILITIES CAUSE DOWNTIME

From 2000 to 2005, reported vulnerabilities increased over 90%

From 2000 to 2005, reported security breaches as a result of vulnerabilities increased 10x (tenfold).

95% of all security breaches result from known vulnerabilities and misconfigurations (Source: 2004 Ecrime Survey, CSO Magazine and CERT)

2. CORPORATE NETWORKS ARE NOW DYNAMIC, MOBILE AND WIRELESS, CREATING MORE RISK

According to Forrester Research, 35 million remote users this year (2005) and 14 billion devices on the Internet by 2010. The need to quarantine high risk, vulnerable systems or untrusted malicious insiders in complicated non-homogenous networking environments is growing dramatically.

3. LACK OF DUE CARE AND DUE DILIGENCE IS VERY COSTLY

CERT calculates the financial damage from these security intrusions worldwide at around \$15 billion annually. Of the 90 percent of CSI/FBI survey respondents detecting computer security breaches within the last year, 80 percent acknowledged financial losses.

The Solution- A Turnkey Vulnerability Management, Regulatory Compliance and Endpoint Security Auditor

NetClarity and its Channel Partners are the exclusive worldwide providers of our patented Vulnerability Management, IT Compliance and Endpoint Security appliances and services.

Auditor™ XL is a network asset defender system in what we believe to be the next wave of Information Security - truly solving your security breach, downtime and out of compliance dilemmas. Auditor™ XL complements all of your recently purchased network traffic defender systems - Firewalls, VPNs, SmartSwitches, Anti-virus, Anti-spam, Anti-spyware gateways, IDS and IPS. With NetClarity's Auditor you will gain:

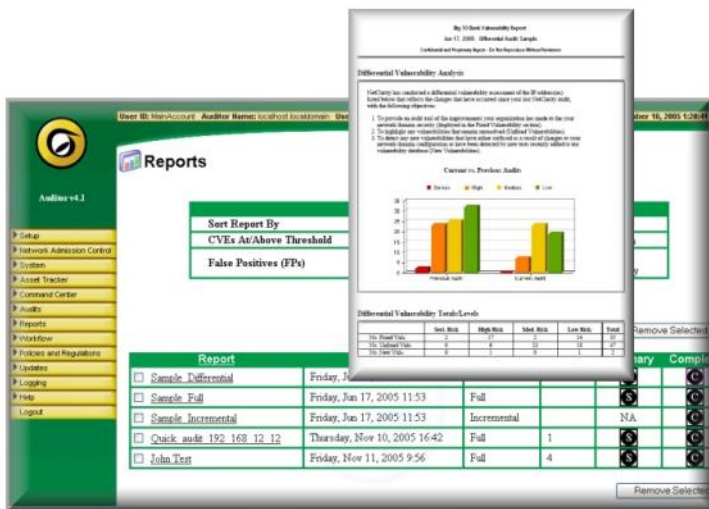
- **PREEMPTIVE: NETWORK ASSET AUDITING**
Audit your network before a hacker does. Generate your own IT Gap Analysis and Regulatory Compliance reports tailored to your industry including Health Care, Insurance, Banking, Retail, Pharma, Government and International standards.
- **PROACTIVE: FIND AND FIX HOLES**
Find all of your common vulnerabilities and exposures with pinpoint accuracy. Clean up and harden network assets for reduced risk of downtime and successful exploiters.
- **PROTECTION: VULNERABILITY QUARANTINE SYSTEM (VQS™)**
Automatically quarantine malicious insiders, weak or untrusted assets, rogue wireless devices and dirty laptops — without ever having to install and manage a client or 'agent' on each system. This is a one of a kind patented solution. It uses your existing firewalls and smart switches to create a safer networking environment and buy you critical remediation time. VQS™ blocks ports and problems not people and productivity. With built-in e-mail alerting and paging.



Secure, Turnkey, Plug-and-Play Appliance

With our uniquely easy to use solution, you will be up and running in five minutes. Within your first hour, you will be productive performing network audits, self assessments and generating reports, automatically, saving you tens of thousands of dollars in consulting fees, time and energy.

- Plug it in, turn it on.
- Connect to it securely, with standard web browser using HTTPS (SSL)
- Log in, find your network assets.
- Schedule your audits.
- Cleanup your holes while you start using the vulnerability quarantine systems.



Key Features

- Vulnerability Management Automation
 - Identify, Track and Log Network Assets
 - Finds and Reports on Thousands of possible weaknesses (CVE@s) through a non-invasive Audit
 - Quarantine Dirty, Weak or Untrusted Systems
 - Cleanup and Harden Trusted Network Assets
- IT Compliance Automation
 - Generate Regulatory Compliance Gap Analysis and Differential Compliance Reports
 - Self assessment, auditing and policy builder tools for VISA/MasterCard PCI, GLBA, HIPAA, CFR21-FDA-11, SOX-404, EO13231, Gov. and International (ISO17799) compliance.

Front:



Rear:



Appliance Specifications

- 800 MHz VIA Eden processor (or higher).
- 4 GB of built-in high speed CF storage (or higher).
- 256 MB of high speed memory (or more).
- Built-in USB and serial ports for initial setup.
- One Internal 10/100 Ethernet controller (NIC).
- Dimensions: 1.18"H x 8.27"W x 5.23"D. (30 mm x 210 mm x 150.6mm).
- Smaller than a paperback - weighs only 3lbs.
- Audits smaller branch or remote office networks and subnets up to 10 IP Addresses.

System Requirements

Works with any Web browser running HTTPS (SSL) including Opera, Internet Explorer, Netscape and Firefox. Can be easily managed through the Auditor Enterprise™ Command Center dashboard.

Benefits

With Auditor Enterprise, you will be able to quickly and easily find all of your Common Vulnerabilities and Exposures (CVE@s) - The root cause of network downtime. All hackers, worms, viruses and spyware use CVE@s to break into your network, behind your firewall.

- Protect Your Assets
- Defend Your Network
- Comply with Regulations

The built-in patented clientless Vulnerability Quarantine System (VQS™) is a ZeroFootprint™ solution.

The VQS™ works with most existing firewalls and smartswitches to *block problems at ports, not people and productivity.*