



Auditor Enterprise



"Very good, fast, powerful endpoint security compliance tool that does what it does very well."
SCMagazine - Group Test - Enterprise Appliances - November 2005

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™ Enterprise 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™ Enterprise 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:

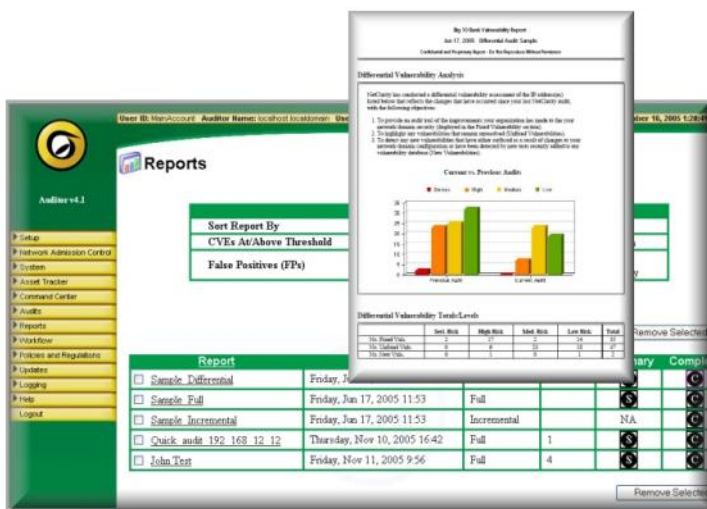
- **PREEMPTIVE: NETWORK ASSET AUDITING**
Audit your network before a hacker does. Generate your own IT Gap Analysis and Regulatory Compliance reports tailored to your industry including Health Care, Insurance, Banking, Retail, Pharma, Government and International standards.
- **PROACTIVE: WORKFLOW AND REMEDIATION**
Schedule remediation, while tracking your progress including time to closure and cost of resource allocation.
- **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 International Email alerting as well as cell phone and pager (SMS) alerting for the USA and Canada.



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.
- Set up the workflow and 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.



Appliance Specifications

- 2.5 GHz Pentium 4 processor (or higher).
- 40 GB of built-in high speed HD storage (or higher).
- 1U rack mountable chassis with universal rails included.
- 1 GB of high speed memory (or more).
- Built-in keyboard, video, mouse and serial ports for initial setup.
- Dual Intel 10/100/Gigabit Ethernet controllers (NICs).
- Audits networks from hundreds to thousands of IP Addresses.

System Requirements

Works with any Web browser running HTTPS (SSL) including Opera, Internet Explorer, Netscape and Firefox.

Benefits

With Auditor Enterprise, you will be able to quickly and easily find all of your Common Vulnerabilities and Exposures (CVEs®) - The root cause of network downtime. All hackers, worms, viruses and spyware use CVEs® 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.*