

DATASHEETS



SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

EXTERNAL NETWORK AUDITING

Auditor LIVE™

BRANCH NETWORK AUDITING

Auditor Branch™

INTERNAL NETWORK AUDITING/NETWORK ADMISSION CONTROL (NAC)

Auditor Enterprise™

ENDPOINT DEFENSE/REAL-TIME NETWORK SECURITY

Protection for Windows™

"It sounds like *NetClarity plans to revolutionize network security ... you may want to keep an eye out for these guys.*" Security Pro News, December 2005

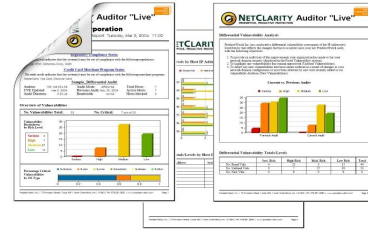
"Beginning from the superb documentation and ending with the high value for the money, this product shines." - *SC Magazine, February, 2006*

"NetClarity picks up where firewall, anti-virus, intrusion detection and intrusion prevention leave off ." - *John Gallant, President, NetworkWorld, May, 2006*

CRN Names NetClarity one of the Who's Who of NAC – "gives Microsoft and Cisco a run for their money." - *CRN, June, 2006*



Auditor LIVE Services



The Problem: Your network may not be secure

You're vulnerable. Malicious attacks are on the rise and information is leaking from your organization. You don't know where or why it's happening.

Phishing, pharming, and information leaks are widespread concerns for many companies from financial institutions to insurance companies to health care providers and public companies.

Costs to hire a large consulting firm to evaluate your security implementation far outweigh the value of the services. You had nowhere else to turn – *until now!*

NetClarity™ Solution: External, Security Assessment Services

NetClarity can assist with your security implementation. Try our turnkey, external, Security Assessment Services for Vulnerability Management and Information Disclosure!

We'll show you where and how to harden your external brand, image, and security posture, and we'll help you comply with stringent government regulations.

NetClarity and our Channel Partners are exclusive worldwide providers of this powerful service based on our award-winning **Auditor** Enterprise appliances and proprietary security services.

Typically, a security assessment of this caliber could take up to one month and cost over \$100,000.

NetClarity **Auditor LIVE** Services offer these types of assessments for a fraction of the cost and in five business days or less! And, you get a comprehensive, confidential 100-400-page report on your external security and compliance posture.

Isn't it time you had a more comprehensive, holistic view of threats, vulnerabilities, external network access, phishing, pharming, and information disclosure?

What are Auditor LIVE Services?

Auditor LIVE is an External, Security Assessment Service that consists of four components. **Auditor LIVE** helps you reduce risk and keeps your network safe from today's dynamic and evolving security threats. Key features include:

Anti-Phishing & Anti-Pharming Sweep

- Finds "knock-off" web page content as soon as it emerges on the web
- Locates site imitators infringing on corporate identities
- Detects duplicate pages with non-identical addresses and summarizes web page contents
- Tracks suspicious email solicitations and correlates with website sweep data

Website Review

- Tests strength of access controls for internal and external websites
- Places special emphasis on information security for electronic commerce
- Evaluates links, URLs, and transport protocols such as HTTP, SHTTP, and SSL

Network Perimeter Discovery and Information Disclosure Sweep

- Reveals confidential information that may compromise security and integrity of a corporate website or intellectual property
- Includes vulnerabilities revealing inside knowledge potentially allowing an attacker to find and exploit other vulnerabilities

External Vulnerability Assessment

- Evaluates strength of current security defenses from internal and external perspectives
- Conducts a series of non-destructive probes manually
- Focuses on system access and configuration controls, password files, Windows® Registry, and NetWare® bindery information.

Auditor LIVE Components

Anti-Phishing & Anti-Pharming Sweep

The Auditor LIVE Website Anti-Phishing & Anti-Pharming Sweep provides corporate web site monitoring using proprietary site sampling techniques.

Auditor LIVE finds web page content that is a “knock-off” of the monitored corporate site. These copycat sites usually originate overseas and are typically involved in various cyber crime activities such as identity or intellectual property theft.

Sweeps detect duplicate pages with non-identical addresses and summarize web page contents for the returned results. Auditor LIVE also tracks suspicious email solicitations and correlates that with website sweep data.

Auditor LIVE performs a review of Global Top Level Domains (gTLD) and Country Code Top Level Domains (ccTLD), any new registrations, and activations or changes to sites that may have suspicious properties.

This component includes functions that automatically track page changes and updates for the current online status of infringing sites. Auditor LIVE also provides corporate site route checking that maps routes to and from multiple locations throughout the world. This process reveals site misdirection techniques using DNS hijacking or cache poisoning techniques.

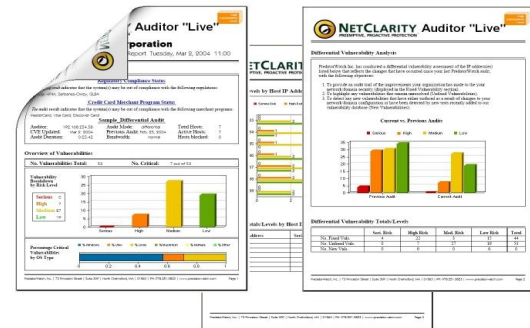
Auditor LIVE reports provide summary and detailed information typically displayed in the following categories. Others may be added or substituted based on findings.

- Duplicate Web site and page detection
- Suspicious email content review
- gTLD and ccTLD review with site registration change tracking
- Imitator site online status and site contact information
- DNS & route analysis from multiple worldwide locations to corporate site(s)
- “Cousin Searches” for mistyped URLs infected with malware
- Search-engine poisoning including imitator websites infected with malware
- Recommended actions in the event of positive imitator detection

Website Review

The Auditor LIVE Website Reviews utilize active and passive security tools designed to identify a variety of security vulnerabilities including:

- Improper access control configurations
- Insufficient or non-existent passwords
- Improper system and network integrity
- Operating system & application software updates & patches



Network Perimeter Discovery and Information Disclosure Sweep

This report provides summary and detailed information typically displayed in the following categories. Others may be added or substituted based on sweep results.

- Availability of published website analysis data
- Links that by-pass protected web pages without login/authentication mechanisms
- Advertised jobs looking for specific skills with technology and tool preferences
- Details on development tools and libraries used to build proprietary applications
- Descriptions of usage problems with development tools and libraries that might show release levels of current technology choices
- Posted system or network configuration data, e.g. ports used, IP addresses, logical network maps
- Descriptions of tools used to manage or monitor systems
- Email addresses that may be used to find further details about employees and contractors or commit spoofing or masquerading attacks against the website
- Descriptions of techniques in use for security and integrity detection mechanisms

External Vulnerability Assessment

The most critical component in any good security program is the establishment of policies and procedures for use of external systems and network resources. Such guidelines are frequently under construction due to changes in business operations, rules, technology, or other variables in the environment.

For additional information about Auditor LIVE or other offerings, contact NetClarity, Inc.

Phone: 781-276-4555
email: sales@netclarity.net
Web: www.netclarity.net



Awarded Five Stars:



Auditor Branch

"Beginning from the superb documentation and ending with the high value for the money, this product shines."

SCMagazine - Group Test - Vulnerability Management - February 2006

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 do they help you comply with government regulations. In addition, none of these solutions can properly alert, block and remediate against dirty laptops, untrusted and malicious insiders or 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: 2005 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.

"NetClarity picks up where firewall, anti-virus, intrusion detection and intrusion prevention leave off."

- John Gallant, President, NetworkWorld - May, 2006

The Solution- A Turnkey Vulnerability Management, Regulatory Compliance and Endpoint Security Branch Auditor with built-in NAC

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

Auditor™ Branch is a network asset defender system for the next wave of Information Security - truly solving your security breach, downtime, and out of compliance dilemmas. Auditor™ Branch 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™ Branch you 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: CLIENTLESS NAC**

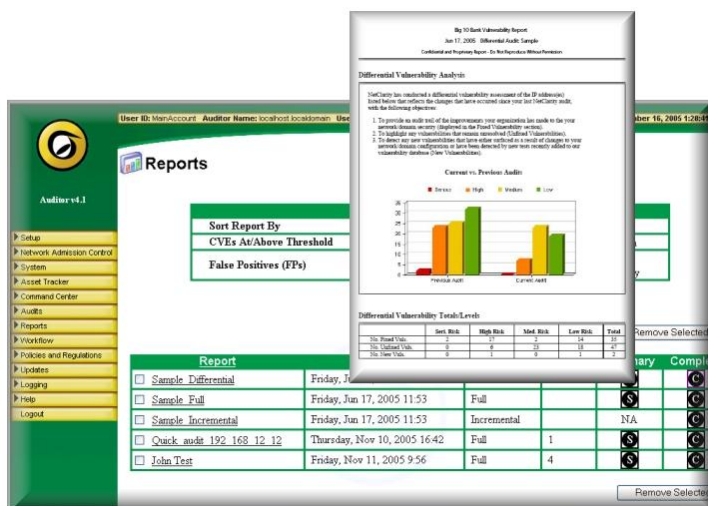
Automatically quarantine malicious insiders, weak or untrusted assets, rogue wireless devices and dirty laptops — without ever having to install and manage a client or 'agent' on each system. This is a one-of-a-kind patented solution. It uses your existing firewalls and smart switches to create a safer networking environment and buy you critical remediation time. The streamlined clientless NAC blocks ports and problems not people and productivity. Includes built-in e-mail alerting and paging at no extra charge.



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 including the Latin American banking standards.
 - Self assessment, auditing and policy builder tools for VISA/MasterCard PCI, GLBA, HIPAA, CFR21-FDA-11, SOX-404, EO13231, Gov. and **International (ISO27001/17799) compliance.**



Appliance Specifications

- 1.4 GHz VIA Eden processor (or higher).
- 40 GB of built-in high speed HD storage (or higher).
- 1 GB of high speed memory (or more).
- Built-in keyboard, video, mouse and serial ports for initial setup.
- One Internal 10/100 Ethernet controller (NIC).
- Dimensions: 8.6"W x 8.6"D x 2.4"H (225 x 225 x 63 mm).
- Size of a paperback book.
- Audits small to medium size networks and subnets up to 256 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 Branch, 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 Network Admission Control (NAC) system is a ZeroFootprint™ solution - no agents or clients need be installed.

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

AVAILABLE NOW:

Call 781-276-4555

Email

sales@netclarity.net

www.netclarity.net



Awarded Five Stars:



Auditor Enterprise

"Beginning from the superb documentation and ending with the high value for the money, this product shines."
SCMagazine - Group Test - Vulnerability Management - February 2006

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 do they help you comply with government regulations. In addition, none of these solutions can properly alert, block and remediate against dirty laptops, untrusted and malicious insiders or 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: 2005 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 with built-in NAC

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 for 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 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: CLIENTLESS NAC**

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. The streamlined clientless NAC blocks ports and problems not people and productivity. Includes built-in e-mail alerting and paging at no extra charge.

"NetClarity picks up where firewall, anti-virus, intrusion detection and intrusion prevention leave off."

- John Gallant, President, NetworkWorld - May, 2006



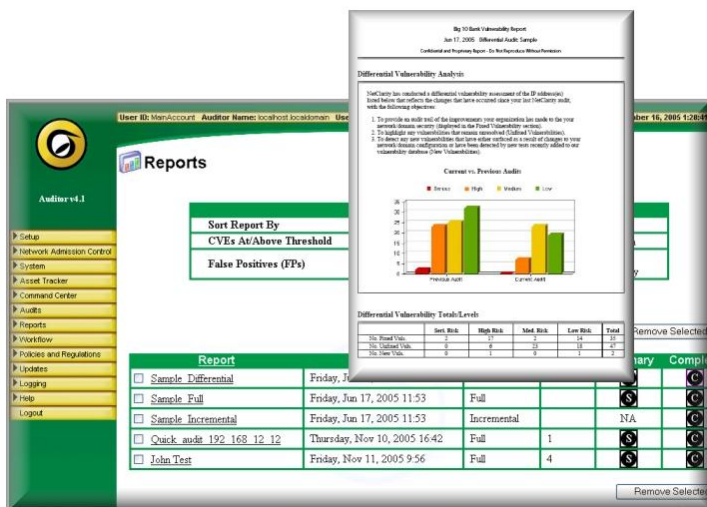
NETCLARITY

PREEMPTIVE, PROACTIVE PROTECTION™

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 including the Latin American banking standards.
 - Self assessment, auditing and policy builder tools for VISA/MasterCard PCI, GLBA, HIPAA, CFR21-FDA-11, SOX-404, EO13231, Gov. and **International (ISO27001/17799) compliance.**



Appliance Specifications

- 2.5 GHz Pentium 4 processor (or higher).
- 80 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 i nto your network, behind your firewall.

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

The built-in patented clientless Network Admission Control (NAC) system is a ZeroFootprint™ solution - no agents or clients need be installed.

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

AVAILABLE NOW:

Call 781-276-4555

Email

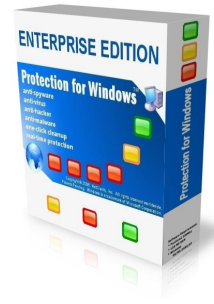
sales@netclarity.net

www.netclarity.net

Reclaim your Microsoft® Windows® Servers, Desktops and Laptops – Free up to 95% of your CPUs



Protection for Windows™ ENTERPRISE EDITION



Self-defending, Self-healing **Windows® Desktop Security** in a complete, easy to use package.
Point. Click. Secure. Includes:

- ✓ **Anti-virus,**
- ✓ **Anti-spyware,**
- ✓ **Anti-hacker,**
- ✓ **Anti-malware,**
- ✓ **Kills rootkits and trojans**
- ✓ **Stops Zero day attacks**
- ✓ **Tamper resistant**
- ✓ **One-click cleanup**

You take countless precautions, but hackers, viruses, worms, spyware, Trojans, adware, keyloggers, backdoors, blended threats, and rootkits are attacking your Windows® desktops and laptops every day.

The anti-virus and anti-spyware software you use is not working – it's only draining your organization. Employees are not productive and your systems are crawling.

How do you significantly minimize the risk these intruders bring to your organization?

Real-time Protection for Windows that works

Protection for Windows™ ENTERPRISE EDITION is a personal computer security monitor that guards against infiltration of unwanted malware programs on your systems.

Protection for Windows is "Self-Defending" and cannot be stopped by hackers or malware. It runs quickly, using little memory and does not impact user productivity and effectiveness.

Whether you're managing a large, complex network, multiple systems on a LAN/WAN, or a SOHO environment, Protection for Windows provides an unparalleled solution for safeguarding the integrity of your information and systems.

Protection for Windows ENTERPRISE EDITION runs in the background using less than 5% of the CPU for minimum impact on system performance.

It installs quickly and easily with a standard Windows installer. You maintain the system from a menu-driven GUI, and it alerts you automatically via on-screen messages or optional email and pager.

Key Product Highlights

- Optionally blocks USB ports and CD/floppy usage
- Prevents installation of unauthorized software
- Detects and quarantines keyboard loggers, remote access Trojans, surveillance tools, NT rootkits, adware, and spyware
- Blocks adware, trackware, spyware and other unwanted websites
- Discriminates between usage errors and unauthorized access
- Rejects illegitimate program termination attempts

Business Benefits

- Enforces uniform, network-wide security policy
- Safeguards corporate resources, prevents data theft
- Mitigates risk and exposure across the network
- Provides cost-effective, continuous protection

Platform Requirements

Multi-platform support for Microsoft™ Windows Operating Systems. Protection for Windows operates on Windows NT, 2K, XP & 2003 platforms with as little as a 300 MHz CPU speed, and less than 256 MB RAM. It takes little disk space and requires less than 15 MBytes free disk space to operate.

Protection for Windows™ - ENTERPRISE EDITION

Retails for \$99.00 USD per PC. Order before December 31st for special introductory pricing of \$59.95/PC.

Contact: NetClarity, Inc.

Phone: 781-276-4555 email: sales@netclarity.net

Corporate Website: www.netclarity.net

Product Website: www.protectionforwindows.com