



PredatorWatch Auditor™

for *Network Security Professionals*

Auditing for Hacker Protection and REGULATORY COMPLIANCE with FDIC, GLBA, NCUA, FDA, and HIPAA

Because your customer's data needs to remain secure. Government regulations demand it.



World's Most Compact Security Appliance with Compact Monitor, Keyboard & Printer

The number of known network vulnerabilities to hacker attack continues to rise—along with regulatory concern about data security. That's where you come in.

Carry in your Security Professional's Auditor in its compact case with monitor, keyboard, and printer.

Scan the customer's network against the federally funded data repository of Common Vulnerabilities and Exposures (CVE®s).

Deliver a report on network vulnerabilities.

Implement click through remedies on the spot.

The PredatorWatch **Auditor**™ cost-effectively performs audits for you, by routinely testing for CVEs in any network. It then provides Administrator reports with remedies for discovered vulnerabilities.

And **Auditor**™ keeps those reports about the network's vulnerabilities inside the customer's network, where they can remain confidential.

Effective security requires defenses for customer-specific vulnerabilities. Firewall and VPN vendors are already designing their products to use **Auditor**™ results to adapt in real time.

GLBA Compliance

The Gramm Leach Bliley Act of 1999 (15 USC 6801-6809) mandates risk controls for "*foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or ... information systems,*" such as:

- Authentication of user identity (passwords, tokens, or biometrics)
- Access controls (limiting certain data to certain users)
- Encryption of sensitive data
- Firewalls between your network and the Internet

However, these controls can be circumvented by attacks that exploit vulnerabilities in networks.

Compliance with FDIC Audit Rules

PredatorWatch **Auditor**™ generates an audit trail to prove that customers have exercised due care in data protection.

Integration with Other Systems

Auditor is designed to work with security counter-measures, such as firewalls, so vendors can customize

their product settings with **Auditor**™ results.

Your Reports Stay Inside Your Network

Reports on customer internal vulnerabilities should remain internal — and confidential. **Auditor**™ doesn't post those vulnerabilities on anyone's Internet web site, "secure" or otherwise.

PredatorWatch Auditor™

the Vulnerability Assessment Appliance

The 1U-A Scans from 3 to 256 IP Addresses

Fits in the palm of your hand.

PredatorWatch Auditor™ Features

Quick Startup—Plug-and-Play

- Plug-and-Play appliance, sets up in 5 minutes
- Delivers results in less than 30 minutes
- Automatically detects IP addresses to scan
- No programming required; ready to run out of the box
- Web-based console using SSL for secure IT admin access
- 10/100/1000 Ethernet ports with auto-sense capability (cross-over or straight cable)
- Autodownload or one-click vulnerability test updates

High Performance Scans

- Continuously audits all of your equipment—servers, workstations, firewalls, routers, hubs, and switches
- Scans into SQL databases, Web server, and email servers
- Detects and lists all open ports, other network info in reports
- Configured for maximum performance and reliability

Operates with Any OS

- Operating System independent—No special OS settings required
- Scans all commercially available operating systems (DOS, Windows, Linux, UNIX, Cisco OS, and others)

Tests Both Systems & Services

Systems and services include:

- | | | |
|----------------|-------------|----------------------|
| ■ bind | ■ NetBIOS | ■ SSH |
| ■ BGP | ■ NIS | ■ SSL |
| ■ CGI | ■ Novell | ■ TCP |
| ■ DHCP | ■ OSPF | ■ telnet |
| ■ CPMA | ■ PPP | ■ TFTP |
| ■ DNS | ■ passwords | ■ users/
accounts |
| ■ DoS exposure | ■ POP3 | ■ Firewalls |
| ■ FTP | ■ proxy | ■ Routers |
| ■ GSM | ■ registry | ■ WAP |
| ■ GSR/RSP | ■ rlogin | ■ UDP |
| ■ HTTP | ■ RPC | ■ VoIP |
| ■ ICMP | ■ RSH | ■ VPNs |
| ■ IMAP | ■ SMB/CIFS | ■ Windows |
| ■ Kerberos | ■ RIP | ■ UMTS |
| ■ LDAP | ■ SMTP | ■ UNIX |
| ■ Linux | ■ SNMP | |
| ■ MLPS | | |

The Auditor™ Edge

Scan-on-Demand—Auditor performs network subnet, computer, server, and device scans on an immediate, daily, weekly, and/or monthly basis—you decide.

Non-intrusive Scanning—Auditor Engine deploys scanning and penetration testing techniques that are non-intrusive.

Turnkey Solution—Simple to install and operate. Integrated software on best-of-breed hardware, with Web-based point-and-click administration, backed by a self-healing & dynamically updating engine.

Proactive Vulnerability Assessment Engine and Database—Auditor leverages real-time, state-of-the-art Common Vulnerabilities and Exposures (CVE) database (maintained by Mitre Corporation). **Auditor** automatically updates as new vulnerabilities arise.

Tamperproof

- Hardened Linux OS in the appliance

Hardware Options

- Runs standalone inside the network
- Portable or 1U and 2U rack mount appliance options

Flexible Configuration Options

- Allows you the option of selecting IPs manually
- Special "Quick Ping" feature indicates availability of target systems

Benefits of Configuration Options

- Variable intensity of testing allows you to customize network load
- Configuration options eliminate false positives, help you stop fighting fires
- Non-restrictive licensing eliminates administrative overhead
- Automated vulnerability assessments free your team from routine IT tasks

Vulnerability Assessment Features

- Regular assessment and reporting provide evidence of diligence in a network security audit trail
- Assessment and reports provide the basis for security policy/risk management program

Auditor™ Reporting Features

Generates Reports on Three Levels:

- **Executive Report** — Succinct, graphical representations. Highlights priority needs.
- **Management Report** — Arms you with info needed to allocate network security investments.
- **Network Administrator Report** — Furnishes classifications, technical info on vulnerabilities, live links to fixes, patches, updates.
- Separate password access to Executive and Management reports
- Custom comment any vulnerability in a report—comments carry forward to the next scan result
- Sort report content by test number or IP address