

the Web Security report

A MESSAGING MEDIA PUBLICATION • NOVEMBER 2006 EDITION • WWW.WEBSECURITYREPORT.COM

ABOUT THIS PUBLICATION

The Web Security Report acts as a publishing partner for Internet security solutions providers, testing labs, research entities and trade organizations. Published monthly by Messaging Media, LLC, the Web Security Report has an online and print audience of over 120,000 readers
publish@websecurityreport.com

TABLE OF CONTENTS

IronPort vs. Bluecoat Product Shootout	1
Web Security News	8
Sponsor Profile	10
In This Edition	12

NETWORK TESTING LABS REVIEW

1106

IronPort S650 vs. Blue Coat Proxy SG8000

Choosing the best protection against spyware.

By Barry Nance

Good anti-spyware defenses are as critical as anti-spam and anti-virus protection. Desktop-based approaches that clean the client, after the fact, are a nightmare to administer. Stopping spyware via gateways at each Internet connection point is clearly superior to cleaning it off individual servers and desktop computers. A gateway is simpler to administer, users can't fool with it and desktop machines and servers don't have to shoulder the extra burden of detecting and removing spyware. To the extent a gateway filters every single crumb of spyware and users do not bring freeware or shareware software into the office, the gateway approach is an ideal way to combat spyware.

To find out which anti-spyware product is best, we tested IronPort Systems' new IronPort S650 Web security appliance and a combination of Blue Coat's SG8000 proxy device and AV2000 scanning device—both in our Alabama lab and at customer sites. The most important criteria in our evaluation was the ability to identify and thwart all (or virtually all) spyware. We also looked for

The IronPort S650 Web security appliance emerged from our testing as the more accurate, higher performance, and easier to use appliance. The IronPort S650 wins the Network Testing Labs World Class award for gateway-based Internet security.



> continued on page 2

in the next issue

What Have We Done? The Internet As Global Critical Infrastructure. Provocative, insightful and educational commentary about the security and scalability of the Internet. Contributors to this feature include representatives from technology companies, trade associations, research groups and the Federal government.

Regular features include: Web Security News, Company Spotlight and Sponsor Profile.

SPONSORED BY
WEBROOT® SOFTWARE





Figure 1: IronPort S650 Web Security Appliance

useful reports, timely alerts, ease of use and ease of deployment. Our goal was to protect our network from malware infections of users' desktops during the regular course of surfing the Web.

The IronPort S650 Web security appliance is exactly what enterprises have been looking for—a fast, accurate, robust, comprehensive, easy-to-use and scalable answer to keeping malware from infecting your network. It excels at thwarting malware by both securing end-user Web surfing and detecting machines inside your network that may have been infected through other means—without hindering or slowing clients' Internet access.

Keeping Malware at Bay

The IronPort S650 Web security appliance operates in one of two modes, securing your Internet traffic (transparent to end-users) by plugging into the appropriate traffic redirection port on a switch or router, or operating as a full forward proxy for



Figure 2: Blue Coat Proxy SG8000

HTTP traffic. In addition, the IronPort appliance integrates a Layer 4 Traffic Monitor (L4TM) that can scan outgoing network traffic across all ports. The combination of the L4TM and the easy-to-deploy transparent mode offers a unique “audit” feature, which will provide you with a full report of malware activity (both going in and coming out of your network) with no major reconfiguration of your infrastructure. When operating, in both transparent and forward proxy modes, the unit adds the ability to do deep content scanning on objects coming back from the Internet—providing full security against remote threats. IronPort uses the Webroot malware scanning engine and signature database for deep content scanning.

In contrast, the Blue Coat Proxy SG8000 unit filters Web traffic for previously known malware URLs and IP addresses, while the companion AV2000 scanning unit subjects Web traffic executable files to deep analysis in order to detect malware. Table 1 shows the malware recognition success rates of the IronPort and Blue Coat devices.

SOLUTION	SUCCESS RATE
IronPort S650 Web Security Appliance	98% (196 of 200)
Blue Coat Proxy SG8000	69% (138 of 200)
Additional Results:	
Blue Coat Proxy SG8000 + Active Controls	80% (160 of 200)
Blue Coat Proxy SG8000 + Active Controls + AV2000 Scanning Device	92% (184 of 200)

Table 1: “Success Rate” is measured as the ability to stop malware (against a suite of 200 malware instances).

	IRONPORT S650 WEB SECURITY APPLIANCE	BLUE COAT PROXY SG8000 & AV2000
Latency (non-executable)	15 ms	22 ms
Latency (small executables, under 256K)	19 to 42 ms	60 to 95 ms
Latency (large executables, over 256K)	5 to 11 ms	135 to 170 ms
Latency (out-of-band scanning)	0 ms	Not Available

Table 2: Latency (performance) results.

Detecting Infections

Stopping malware at the gateway is only one part of the equation. There are numerous other vectors for infection that often aren't under IT's control. For example, roaming laptops will often become infected when browsing the Web from an employee's home or while on the road. When these malware carriers come back to the corporate network, the first thing the Trojans will do is try to contact their command center, an activity also known as "phoning home". IronPort's S-Series appliances include the unique addition of a traffic monitor that scans all outgoing Layer 4 network traffic for this phone home activity and reports on the internal systems this traffic emanates from. This helps administrators quickly identify end-user computers that may be infected with spyware.

Performance

The speed with which a Web security gateway product processes Web traffic governs the responsiveness that users experience as they browse the Internet. Even the most accurate Web security tool is useless if it slows Internet responsiveness to the point of user frustration. Table 2 reveals the performance of the IronPort S650 gateway and the combination of Blue Coat's SG8000 and AV2000 devices. To perform deep content scanning on objects being retrieved from the Web, the Blue Coat SG8000 must download

the file, send it over the network to the AV2000, and then wait for a scanning result before proceeding. The IronPort S650 offers an innovative architecture that allows it to begin transmitting large objects back to a requesting client—even before the entire object has been received from the remote site and scanned. This made the IronPort S650 the faster of the two for all scanning activities, and remarkably faster for objects of more than 256K. IronPort calls this new archi-

Technology Innovation

Phone Home Scanning

Clients can become infected with malware through many vectors other than HTTP (such as from other compromised systems at a public Wifi hot spot). When a Trojan downloader is installed, it will attempt to connect to an illicit server in the network and download other malware — an activity known as "phoning home". Detecting clients infected with malware by scanning for phone home activity is critical.

IRONPORT	BLUE COAT
Scans all ports for known malware bypassing Port 80 using integrated Layer 4 Traffic Monitor	Monitors outgoing HTTP to malware sites
Rating: A	Rating: C-

> continued on page 4

structure its Dynamic Vectoring and Streaming (DVS) engine. In addition, when configured to scan Web traffic out-of-band in transparent mode, the IronPort introduced no latency into users' network traffic.

In our accuracy and performance tests, we used fresh material for each test to negate the effects, if any, of caching by the gateway devices.

IronPort uses the concept of "Web Reputation" to greatly increase the security and speed by which it executes Web-based scanning. Based on historical malware activity and traffic data collected from numerous sources, IronPort derives a "reputation score" for various Web hosts, URLs and IP addresses. This data is gathered by IronPort's SenderBase Network monitoring system, which provides reputation data for both email and Web security. The IronPort S-Series uses reputation data to determine the relative risk of different sites and objects that a user is requesting. This approach can accelerate the end-user experience by blocking known bad sites outright, performing further scans on any content from unknown or suspicious hosts and allowing content from known good URLs to

pass through, unimpeded. Using reactive URL lists has been common in Web security for quite some time (the Blue Coat units similarly use white lists and black lists to approve or block specific website visits), but IronPort's technology is the first preventive solution that tracks and updates reputation scores in real time—increasing security and accuracy for its customers.

Content Scanning

The IronPort S650 achieves its quick yet powerful transparent mode results by issuing a TCP Reset command to both the client and the spyware host when the IronPort S650 detects malware—effectively telling the client and spyware host to stop talking. This approach is extremely clever and allows the IronPort S650 to thwart malware while letting benign traffic to flow unhindered across the network. Even in deep analysis mode, (using the DVS engine) the IronPort S650, in rather sophisticated fashion, passes all but the last packet to a client. That last packet triggers the IronPort S650's deep analysis of a

Testbed and Methodology

Focusing on these two new gateway products, we primarily looked for the ability to identify and block malware (such as keystroke loggers, browser hijackers, adware, rootkits, dialers, data miners and Trojans). We wanted a product to prevent malware from sending data from our network (i.e., "phoning home"), identify already-infected clients, scan traffic quickly, receive frequent spyware definition updates, integrate with a network management system (such as OpenView) and produce helpful reports on infection attempts and traffic statistics.

We collected a suite of 200 malware samples and moved the collected material to an isolated, quarantined network. We thus were able to simulate the Internet within our lab.

The quarantined network consisted of three subnets.

- **Subnet 1** had 10 client machines with a variety of operating systems, including Windows NT, 98, 2000, ME, XP, Red Hat Linux and Macintosh OS X.
- **Subnet 2** contained three Web servers (Microsoft IIS, Netscape Enterprise Server and Apache), three email servers (Exchange, Notes and Sendmail), two file servers (Windows 2003 Advanced Server and Netware) and two database servers (Oracle 8i and Microsoft SQL Server).

potentially unwanted executable. The IronPort S650 appliance's approach makes sure that the user doesn't have to wait twice as long for a download—once to the gateway and then again to the desktop. Note that the IronPort S650 forwards the last packet to the client only if the executable file is not malware. The IronPort S650 is clearly designed with user responsiveness in mind.

Blue Coat uses two separate appliances to perform deep content inspection. The SG8000 handles data compression, caching proxy functions and URL/IP address recognition. It uses the ICAP protocol to pass files to the AV2000 unit for deeper scanning. The Blue Coat system does not have an out-of-band (transparent) mode, or a Layer 4 Traffic Monitor to detect phone home activity. The only outgoing communication by a malware-infected PC is HTTP-based communication on Port 80. Unfortunately, this means that the Blue Coat system cannot detect clients that are infected by the most recent crop of malware software, which uses sophisticated protocols to retrieve new instructions from the Internet and upload sensitive information.

Vendor Details

IronPort S-Series Web Security Appliance
Price: Starts at \$24,995.00

IronPort Systems, Inc.
950 Elm Avenue
San Bruno, California 94066
(650) 989-6500
www.ironport.com

Blue Coat SG8000 Series Proxy
Price: Starts at \$48,295.00

Blue Coat AV2000 Scanning Device
Price: Starts at \$20,995.00

Blue Coat Systems, Inc.
420 North Mary Avenue
Sunnyvale, California 94085
(866) 982-2628
www.bluecoat.com

Hardware

The IronPort S650 appliance and both the Blue Coat SG800 and AV2000 are all hefty units. The IronPort

—————> *continued on page 6*

- **Subnet 3**, simulating the “Internet,” had Web servers and clients that contained the malware instances and sported “bad guy” IP addresses and URLs. Systems on the first two subnets accessed the third subnet as if it were the actual Internet.

To measure performance, we used two time-synchronized protocol analyzers on the Internet and local network sides of the gateway device and examined the resulting packet captures to know the time taken by a device to forward or discard each network message.

Each gateway product connected our two client subnets to our simulated “Internet”. Client and server machines started off in a pristine state for each test.

Our clients and servers attempted to download malware from the simulated “Internet.” We noted how well the products identified malware traffic and blocked attempts by the malware to send data back to the source. We gauged success or failure by examining each machine for malware after each test. We looked for running malware processes, new program files (EXE, DLL or OCX, possibly marked with the hidden attribute) and directories as well as Registry and Start Menu changes.

S650 has dual Xeon processors, 4 GB of RAM, 876 GB of disk space and a broad range of network connectivity options, including a 1 GB NIC. The SG8000 has a single processor, 2 GB of RAM, 292 GB of disk space and 6 GB Ethernet ports. The AV2000 must be racked near the SG8000 and connected directly to it.

Ease of Use

The IronPort S650 and the Blue Coat SG8000/AV2000 combination each offer browser-based access to the appliances' configuration settings and reporting tools. The IronPort S650's user interface,

which presents a tab-folder metaphor, is the more intuitive of the two solutions and is, by far, the easier to navigate.

The SG8000 and AV2000 appliance combination supplies a central console for managing multiple appliances across a large network. The IronPort S650 lacks a central console, but IronPort says it will be adding this feature in the near future.

Configuring security policies on the IronPort appliance involves selecting which kind of malware you want to block, using high-level categories such as "Keyloggers" and "Adware." The IronPort S-Series also gives you fine-grained control, via Web

Malware Security Report Card

Grade scale is A through F, with A = Perfect and F = Failing

CATEGORY AND WEIGHT (%)	IRONPORT SYSTEMS IRONPORT S650 WEB SECURITY APPLIANCE	BLUE COAT SYSTEMS PROXY SG8000 + AV2000
Preventing malware infections through Web browsing (25%)	A	B-
Detecting clients already infected with malware (15%)	A	C-
Performance (20%)	A	B
Ease of Use (10%)	B	A
Reports (10%)	A	B
Deployment (10%)	A	A
Documentation (10%)	A	A-
Overall Score	A-	B-
Pros	Top-notch malware protection	Full set of HTTP proxy features
Cons	Lacks a central console	Requires two appliances for deep content scanning. Only detects phone home activity over HTTP.

Reputation, to determine which sites and objects you will block outright, scan further, or allow to pass-through.

Blue Coat's anti-malware configuration is more complex. It involves turning on ICAP scanning through the separate AV appliance, setting specific content types to block and enabling the Blue Coat Spyware URL database.

The IronPort S650 also provides a greater range of useful reports than the Blue Coat SG8000. We found that the IronPort S650's reports gave us the clearest picture of malware activity – both in detail (for specific infected clients) and in summary (for the entire network).

In particular, an IronPort S-Series appliance can operate in a convenient "Network Audit" mode, in which it monitors your network traffic through a hub, tap or span port on a switch to provide full reporting on the amount of malware present in your users' Web traffic. IronPort's appliance also reports on all outgoing phone home activity, regardless of port number, from any infected client system.

Both the IronPort and the Blue Coat appliances can integrate via SNMP with a network management system such as OpenView.

Deploying an IronPort S650 or a Blue Coat SG8000/AV2000 combination is easy. It consists simply of cabling the box (two boxes, in the Blue Coat environment) to your network, powering up and assigning an IP address. Cabling varies slightly between the inline and transparent modes.

The IronPort S650 documentation is clear, comprehensive and easy to follow. In contrast, the both the Blue Coat SG8000 and AV2000 documentation use lots of illustrations. But they lack clarifying descriptions of the impact of the various configuration settings as well as clear, unequivocal explanations of the interactions between the two devices.

Conclusion

While Blue Coat's proxy-based protection has worked for companies with basic Web security needs, the evolution of malware demands a new approach that combines deep content scanning, phone home activity detection and very high performance. The new IronPort S-Series offers a unique approach to Web security that combines all the most important services into a single, integrated appliance.

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. You can email him at barryn@erols.com.



About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

DHS Gets \$87 Million for Cybersecurity

On October 4, President Bush signed the fiscal year 2007 appropriations bill for the Department of Homeland Security. The bill provides a total of \$542 million for infrastructure protection and information security, including \$87 million for cybersecurity.

Earlier this year, the Bush administration requested an increase of \$14 million (or 17 percent). Unfortunately, the increase over fiscal year 2006 is only \$8 million, or 10 percent (\$79 million budget for fiscal year 2006.)

What message does this send to cyberterrorists, and even criminally-minded hackers? Critics agree that, even if it is a normal practice in Congress to undercut the administration's budget request, underfunding the budget for protecting a critical aspect of the nation's economy seems unwise.

The full White House press release can be found at: <http://www.whitehouse.gov/news/releases/2006/10/20061004-2.html>

IronPort Honored with Industry Accolade

Info Security Products Guide, a Silicon Valley Communications publication and the world's leading publication on security-related products and technologies, has honored Ambika Gadre, IronPort Senior Director of Product Management, with the Shaping Info Security 2006 Industry Award. This prestigious industry award recognizes individuals and teams worldwide that have made the most positive impact on security technology in today's highly sophisticated environment.

At IronPort, customers approached Gadre and her team to tackle the spyware problem. Though it took significant investment, the IronPort S-Series (the industry's fastest Web security appliance) was developed because of the increased demand from enterprises to stop and combat spyware — one of the most significant corporate security issues today.

To read more about Gadre's contribution to enterprise security, visit: <http://www.infosecurityproducts-guide.com/people/>

Symantec Reports on Internet Threat Activity

Symantec recently released the tenth version of its Internet Security Threat Report, which provides a six-month (January 1 to June 30, 2006) update of Internet threat activity. It includes an analysis of network-based attacks, disclosed vulnerabilities, malicious code reports and security risks. Based on Symantec's expertise and experience, this analysis yields a highly informed commentary on current Internet threat activity.

The current Internet security threat environment continues to be populated by lower-profile, targeted attacks as cyber criminals identify new ways to steal information or provide remote access to user

systems. The attacks propagate at a slower rate in order to avoid detection and increase the likelihood of successful compromise before security measures can be put in place.

By publishing the analysis of Internet security activity in the Internet Security Threat Report, Symantec hopes to provide enterprises and consumers with the information they need to help effectively secure their systems now and in the future.

The complete Internet Security Threat Report is available at: <http://www.symantec.com/enterprise/threatreport/index.jsp>

Hackers Find Use for Google Code Search

Google Inc. has inadvertently given online attackers a new tool. Unlike Google's main Web search engine, Google Code Search peeks into the actual lines of code whenever it finds source-code files on the Internet. This will make it easier for developers to search source code directly and dig up open-source tools they may not have known about, but it has a drawback.

Unfortunately, attackers may also be able to use the new tool to find vulnerabilities in password mechanisms, or to search for phrases within software such as "this file contains proprietary," possibly unearthing source code that should never have been posted to the Internet.

To learn more about Google Code Search, visit: <http://www.google.com/codesearch>

Security's Rotten Apples

If you're working with at least two other IT/security professionals, and you're not breaking any rules, look around—there's a good chance one of them is. That's the net result of Dark Reading's "Security Scruples" reader survey, which tested the attitudes and ethics of some 648 IT and security pros.

The survey, which asked IT people about their beliefs and behavior in both real and hypothetical security situations, suggests that about two thirds of them agree on the conventions for proper conduct—and the other third might be doing anything from peek-

ing at colleagues' personal data to actively stealing information from the company.

Virtually all of the respondents said the key to avoiding ethical problems in IT organizations is to hire the right people. "One of the toughest issues we face right now is doing employee background checks," said one security manager. "Insiders can do the most damage."

More detailed information about this survey can be found at: http://www.darkreading.com/document.asp?doc_id=105282

company spotlight

Internet Security Systems

Internet Security Systems, Inc. (ISS) provides security products and services that preemptively protect enterprise organizations against Internet threats. ISS has commanded the leading edge of security innovation, inventing cornerstone technologies such as vulnerability assessment and intrusion detection/prevention.



The company continues to set standards in the security space with ISS protection platform, offering enterprise-wide preemptive protection that is tightly integrated with existing IT business processes. ISS is headquartered in Atlanta and maintains more than 35 offices in 20 countries worldwide. www.internetsecuritysystems.com

WEBROOT SOFTWARE provides the leading anti-spyware solutions for individuals and organizations around the globe. Enterprises today need to effectively block and remove new and rapidly evolving Internet security threats while minimizing system impact. Spyware and other malicious software is becoming more aggressive and insidious every day, with spyware developers using variations of old tricks to bypass new solutions. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware has become adept at covertly infiltrating a system and installing itself deep within an infected computer.

Defining the Spyware Threat

Webroot's enterprise anti-spyware solutions protect the key entry points (perimeter and desktop) of your network from attack, ensuring your confidential and proprietary assets are safe from external threats. The Webroot enterprise solution comes in two parts:

- RockSafe™ E1000 perimeter anti-spyware on the IronPort S-Series™ appliance—The strongest network anti-spyware solution on the market, focused on detecting and blocking spyware before it can infect the enterprise; and
- Spy Sweeper™ Enterprise—The industry leading desktop anti-spyware solution created to mitigate all spyware threats if they have infiltrated the perimeter through other means such as the use of USB drives or laptops taken off the corporate network.

The Most Effective Anti-Spyware Solution

Webroot Spy Sweeper Enterprise is an award-winning, enterprise anti-spyware solution that provides centrally managed, desktop-level protection. Spy Sweeper Enterprise effectively manages the spyware threat by reducing security risks, minimizing IT help-desk requests, and re-establishing computing and network performance. The Webroot Comprehensive Removal Technology (CRT) is the backbone behind the most advanced spyware removal engine in the industry. This unique technology completely immobilizes spyware detected on a PC. Using CRT, Spy Sweeper Enterprise assures system stability during and after the removal process. Spy Sweeper Enterprise removes and blocks the most persistent spyware programs today.

Gateway Technology: RockSafe E100

While desktop protection is an absolute necessity, utilizing gateway technology to slow the scourge of spyware is also imperative. In fact, most security analysts recommend a layered protection approach when it comes to Enterprise protection from spyware. To fill this gap, Webroot offers the RockSafe E1000 perimeter anti-spyware SDK—the easiest to use, fastest, and most effective anti-spyware engine available for the network appliance OEM market.

RockSafe E1000 provides the core technology for products that monitor traffic at the network perimeter and take appropriate action when a spyware threat is identified. By scanning both URLs and binaries, RockSafe E1000 technology can be used to provide protection for inbound and outbound network traffic. With the comprehensive software, documentation and sample applications included



Phileas™: Webroot's automated spyware research system proactively seeks out malware.

in the RockSafe E1000 SDK, Webroot partners can quickly and easily integrate spyware protection into their network gateway appliances. RockSafe E1000 offers developers fast-track integration while satisfying the requirement of high-bandwidth environments for minimal performance overhead.

Key product benefits include:

- Spyware download URL identification
- Spyware communication URL identification
- Phishing URL identification
- Spyware binary identification
- Malicious ActiveX CLSID identification
- Small memory and disk footprint
- Performance optimized for minimal traffic latency
- Designed for easy integration
- Uses the same industry leading definitions as Webroot Spy Sweeper

Powered by Phileas

RockSafe E1000 leverages the power of Phileas V, the next generation of Webroot's automated spyware research system designed to proactively seek out the most malicious types of spyware and malware, and Webroot's renowned in-house Threat Research Team. Phileas is a groundbreaking online spyware research system developed by Webroot. Using patent-pending technology that scours the entire Internet, Phileas discovers spyware on the Web faster and more efficiently than any other research method. More importantly, it does so before corporations unwittingly become infected.

Using the data culled by Phileas V, Webroot's Threat Research Team has created a comprehensive set of network perimeter signatures that can be used to stop malicious threats before they reach the desktop. With nearly 150,000 of these signatures, RockSafe provides a comprehensive first layer of defense.

Stop Spyware at the Corporate Perimeter

Webroot has recently joined forces with IronPort® Systems Inc., the leader in gateway security, to stop spyware at

the corporate perimeter. IronPort is using the Webroot RockSafe E1000 SDK in the new IronPort S-Series Web security appliances. The IronPort S-Series combines a high performance Web proxy for application layer analysis with a wire-speed Layer 4 Traffic Monitor, yielding the fastest and most comprehensive protection in the industry. The Webroot SDK was built for speed and efficiency and relies on Webroot's extensive spyware definition database to deliver the most effective perimeter anti-spyware engine available. The combination of the high performance IronPort platform and the Webroot anti-spyware software yields a product that

is unmatched in its ability to stop spyware across all network ports for even the largest enterprises. Enterprise IT managers can now deploy a single appliance that contains best of breed technology from multiple vendors, without the administrative burden of managing multiple discrete systems. Product policies and configuration are all set from a single, intuitive, Web-based administration console.

The Webroot/IronPort Partnership

The Webroot/IronPort partnership has resulted in the industry's most accurate Web security appliance. This accuracy is driven by unique technology from both companies. To learn more about how to protect your enterprise from Internet threats, visit www.webroot.com or call 800-870-8102.

The combination of the high performance IronPort platform and the Webroot anti-spyware software yields a product that is unmatched in its ability to stop spyware across all network ports for even the largest enterprises.



www.webroot.com

PAGE 1 IronPort vs. Blue Coat

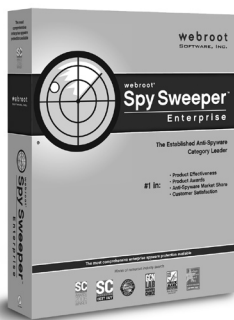
Network Testing Labs and the Web Security Report present the telling results of a head-to-head product comparison of gateway-based anti-spyware solutions.

PAGE 8 Web Security News

Your source for short takes on Web security tales, tools, tips and trends.

PAGE 10 Sponsor Profile

Web Security Report sponsor, Webroot Software, is developing Internet security software to provide customers with privacy, protection and peace of mind.



THE WEB SECURITY REPORT

A Messaging Media Publication

BUSINESS OFFICES

Messaging Media, LLC
P.O. Box 643084
Los Angeles, CA 90064
Phone: 866-808-4200
Fax: 310-836-4067

ADVERTISING/SPONSORSHIP INFORMATION

Managing Partner: Tim Matteson
publish@websecurityreport.com
866-808-4200 (ext. 361)

the Web Security report

Messaging Media, LLC
10536 Putney Road
Los Angeles, CA 90064