

www.securecomputing.com

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.



Web Gateway Security
Protections and Capabilities



URL Filter



Anti-Malware



Anti-Virus



SSL Scanner



Content Reporter



SecureCache

WWPO-01-C

© 2007 Secure Computing Corporation. All Rights Reserved. WW-PO-Jan08vF. Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, SoftToken, Enterprise strong, MobilePass, G2 Firewall, PremierAccess, SecureSupport, SecureOS, Bess, CyberGuard, Total Stream Protection, Webwasher, Strikeback, and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, Security Reporter, Application Defenses, Central Management Control, RemoteAccess, IronMail, SecureWire, SnapGear, TrustedSource, On-Box, Securing connections between people, applications, and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.

Webwasher Products

Security Challenges in a Web 2.0 World

Organizations can do more over the Web today than ever before. As use of the Web continues to grow and evolve with adoption of Web 2.0 applications, virus outbreaks and other forms of Web-borne threats known as “malware” continue to grow as well. Are you adequately protected?

Widely deployed reactive security solutions based on a negative security model of blocking “known bad” behavior and content (such as signature-based anti-virus and category-only URL filtering), while providing vital security, were not designed to combat malicious software code or cleverly blended threats, hidden inside seemingly good HTTP or HTTPS traffic. Furthermore, today’s malware attacks are rarely Web wide, rather they are targeted at individual organizations. While organizations need the Web, they need to be protected from Web-related attacks targeted at them.

The adoption of Web 2.0 applications by the enterprise requires a security solution for Web 2.0. Secure Computing has taken a fresh look at today’s Web security needs and has solved this growing problem: Webwasher® Web Gateway Security appliances.

Web Gateway Security Solution – Webwasher

Webwasher delivers a comprehensive security solution for all aspects of Web 2.0 traffic. When a user is requesting content from a Web 2.0 application, they are implicitly asking for active content to be delivered to, and executed by, their computer. Furthermore, the same user is required to provide content to the Web 2.0 application, making the security concerns both inbound and outbound in nature.

Webwasher provides immediate protection for user-initiated Web traffic against threats such as malware hidden in blended content or hidden in encrypted SSL traffic. Webwasher analyzes the intent of all content entering the network—even new Web pages before they have content and before they are categorized. It also protects organizations from outbound threats such as potential loss of confidential information that can leak out on all key Web protocols (HTTP, HTTPS, and FTP).

Webwasher Protections

- **#1 rated malware protection** – Webwasher Anti-Malware, using proactive intent analysis, filters objectionable content from Web traffic. By scanning a Web page’s active content and understanding its intent or predicted behavior, Webwasher is able to proactively protect against spyware, day-zero, blended threats, and targeted attacks. Anti-virus solutions that solely rely on signature updates or heuristics cannot provide this level of protection. Webwasher combines this threat protection against unknown malware with the exceptional performance of a signature-based anti-virus engine for known malware threats to provide the industry’s best Web Gateway defense against malware as rated by independent studies*.
- **Reputation-based security through TrustedSource** – Secure Computing has set a new standard for proactive detection through our industry-leading reputation system, TrustedSource. Relying on extensive knowledge of Internet entities and the constantly changing global threat landscape, the TrustedSource network identifies potentially malicious behavior and enables organizations to block these threats based on an assigned reputation

* according to PCMag.com article “AV-Test.org Reports Stats from Antivirus Roundup” <http://www.pcmag.com/article2/0,1759,2135092,00.asp> (May 22, 2007)

Web 2.0 Defined

The phrase **Web 2.0** refers to a perceived second-generation of Web-based communities and hosted services—such as social-networking sites, wikis, and folksonomies—which aim to facilitate collaboration and sharing between users....a Web 2.0 Web site may exhibit some basic common characteristics. These might include:

- “Network as platform”—delivering (and allowing users to use) applications entirely through a browser
- Users owning the data on a site and exercising control over that data
- An architecture of participation that encourages users to add value to the application as they use it
- A rich, interactive, user-friendly interface based on Ajax or similar frameworks
- Some social-networking aspects

Wikipedia:
http://en.wikipedia.org/wiki/Web_2.0

score. Webwasher is integrated to the global TrustedSource reputation network to proactively find, report, and block traffic to and from questionable sources. For details, see the TrustedSource whitepaper (<http://www.securecomputing.com/webform.cfm?id=105&ref=1657>)

- **Protection for encrypted traffic** – SSL traffic (HTTPS) is widely seen as the new back door through an organization’s security barrier and must be secured the same way traditional HTTP traffic is secured. Webwasher is the first security product available that fully integrates malware detection, SSL inspection, and certificate validation. There is no need to route traffic to a separate box for malware inspection, as Webwasher scans all SSL traffic on the appliance maintaining the complete security, integrity, and privacy of the SSL transaction.
- **SecureCache** – Secure Computing is the first vendor to rethink the design of proxy/cache specifically for a secure Web 2.0 environment. Webwasher SecureCache™ uses a revolutionary new design that employs proactive scanning and security reputation prior to delivering a cached object to an end-user. This provides much more efficient virus and malware scanning while dramatically reducing the amount of disk storage required compared to traditional caching solutions.
- **Data leakage protection** – Webwasher protects organizations from outbound threats such as loss of confidential information that can leak out on all key Web protocols. Webwasher provides this outbound security by performing unique outbound scanning of content—even content transmitted via SSL. This makes Webwasher an important tool in an organization’s arsenal to prevent intellectual property loss, comply with regulatory requirements, and provide reporting for compliance as well as forensics in the event of leakage. For organizations with advanced DLP requirements, Webwasher is the perfect platform to implement third-party DLP engines.

Webwasher Web Gateway Security Appliances

Webwasher completely integrates numerous protections that would otherwise require multiple stand-alone products, such as URL filter, anti-virus, anti-spyware, SSL scanner, and content control filters in one single and easy to manage appliance. Whether you need to protect your network from spyware and malware, prevent employee access to risky Web sites, or control the dissemination of confidential information via the Web gateway, Secure Computing has a Webwasher solution that fits your budget and your needs.

You’ll start with a high-performance, enterprise strong® proxy appliance that ships with the authentication, administrative, and authorization controls necessary to control Internet access and use. A variety of dashboard reports reveals the current health of the appliance as well as an instant snapshot of the filtering performance. Additionally, all appliances ship with SSL Scanner and SecureCache enabled, the industry’s first and only security aware cache for Web 2.0 powered by TrustedSource global reputation.

Webwasher appliances are preinstalled with a proven default configuration that allows fast, easy, and error-free deployment. Webwasher’s unique Security Shield monitor ensures a secure configuration without loopholes and up-to-date anti-malware and URL data. Policy changes in complex, multi-appliance environments are easy to manage since changes are pushed from a master instance to child instances.

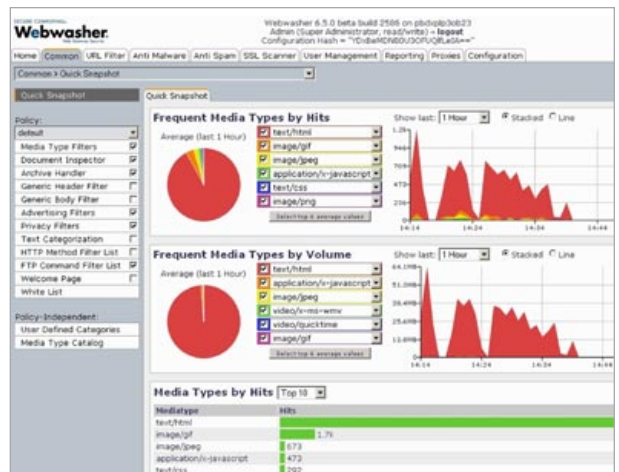


Figure 1: Webwasher security dashboard

Webwasher uses the industry standard ICAP (Internet Content Adaptation Protocol) to efficiently communicate with other security appliances, data leakage solutions, as well as an array of industry standard proxy/caching devices, plugins for Squid, ISA Server, proxy chaining, and the IFP protocol.

Security now extends to Webwasher administration as well. Webwasher supports Secure Computing's SafeWord® two-factor authentication for securely accessing and administering the Webwasher solution.

Webwasher Protection Modules

Webwasher protections are available in different modules so customers can pick and choose the level of defense they want. And because all Webwasher modules are tightly integrated, Webwasher's efficient policy management enables administrators to specify policies once that apply to all modules and are valid for all Web, SSL, and FTP traffic.

Webwasher URL Filter

Webwasher URL Filter combines the accuracy and breadth of the SmartFilter® category-based URL database with reputation-based filtering powered by TrustedSource global intelligence. This combination, unique only to Webwasher, makes Webwasher URL Filter the most powerful filtering solution available today. Webwasher URL Filter prevents malicious content from entering your network and significantly reduces productivity losses, bandwidth consumption, and legal risks caused by unauthorized employee access to inappropriate or distracting Web content. Webwasher URL Filter comes with an easy-to-use drill-down reporting solution so you can easily determine where your employees spend their time on the Web.

Webwasher Anti-Malware

Webwasher Anti-Malware is the best available solution to stop both known and unknown malware including viruses, spyware, and key-loggers from entering your network, even if downloaded within an encrypted SSL session. Webwasher combines the exceptional performance of signature-based anti-virus/anti-malware engine for known malware with the in-depth analysis of our proactive, intent analysis security filters to detect blended or yet unknown bad content with malicious intent. Deep content inspection makes sure that malware is reliably detected even if hidden deep in compressed or spoofed files.



The No. 1 product, Webwasher by Secure Computing, detected 99.83% of 606,901 malicious samples

AV-Test.org Reports Stats from Antivirus Roundup

PC Mag.com, May 22, 2007
<http://www.pcmag.com/article2/0,1759,2135092,00.asp> (May 22, 2007)

Webwasher has been positioned by Gartner, Inc., a premier research and advisory firm, in the Leaders Quadrant of the "Magic Quadrant for Secure Web Gateway, 2007" report published on June 4, 2007.

Leaders are high-momentum vendors (based on sales and "mind share" growth) with emerging track records in Web gateway security, as well as vision and business investments that indicate they are well-positioned for the future.

The Magic Quadrant is copyrighted 2007 by Gartner, Inc. and is used with permission.

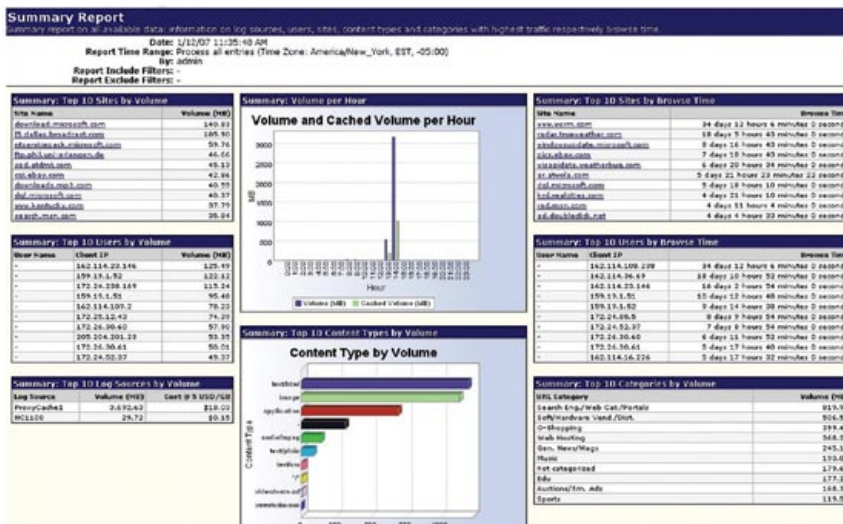


Figure 2: Comprehensive reporting on Web traffic



For more information

Contact your local reseller,
or Secure Computing at:
1-800-379-4944 (inside U.S.)
1-408-979-6100 (worldwide)
sales@securecomputing.com
www.webwasher.com

Secure Computing Corporation

Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.6501

European Headquarters
Berkshire, UK
Tel: +44.(0).870.460.4677

Asia/Pacific Headquarters
Wan Chai, Hong Kong
Tel: +852.2598.9280

Japan Headquarters
Tokyo, Japan
Tel: +81.3.5339.6310

For a complete listing of all
our global offices, see www.securecomputing.com/goto/globaloffices

Webwasher SSL Scanner

Webwasher SSL Scanner fills a serious security gap in the corporate IT wall of defense. Webwasher SSL Scanner denies hackers, viruses, and other malicious content hidden in SSL-encrypted traffic access to your network. By scanning SSL (HTTPS) traffic and providing certificate updates, which most vendors cannot provide, Webwasher enables enterprises to apply all of the advanced Webwasher protection filters, along with their existing security and Internet usage policies to all encrypted traffic.

Webwasher Anti-Virus

For organizations who want additional signature-based anti-virus protection, Webwasher Anti-Virus enables organizations to purchase one of two 3rd-party anti-virus solutions to protect against viruses in Web and FTP traffic at the gateway. Secure Computing can license anti-virus solutions from both McAfee and Sophos to our customers to run on the Webwasher appliance.

Webwasher Content Reporter

Content Reporter provides an in-depth view of the peaks, trends, and events related to all network activity, including cache, streaming media, Web, and email usage. Content Reporter enables automated data collection from multiple sources, simplifying ongoing maintenance and report generation. This highly scalable solution is an excellent reporting application for even the largest global corporations.

Webwasher Appliance Specifications



Model name	WW500C	WW1100C	WW1900C	WW2900C
Form factor	1U rack mount	1U rack mount	1U rack mount	2U rack mount
RAM	2 GB	2 GB	4 GB	4 GB
Processor	Single	Dual core	2 Dual core	2 Quad core
Processor cache	512 KB	2 x 2 MB	4 MB	2 x 4 MB
Disk	160 GB SATA	2 x 160 GB SATA	2 x 300 GB SAS	2 x 146 GB SAS + 4 x 300 GB SAS
RAID	-	RAID 1	RAID 1	RAID 1/RAID 5
Power supply	Single	Single	Redundant	Redundant
Interfaces	2 x 10/100/1000	4 x 10/100/1000	4 x 10/100/1000	4 x 10/100/1000