

## Webwasher products

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 Products



URL Filter



Anti-Malware



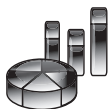
Anti-Virus



Anti-Spam



SSL Scanner



Content Reporter

WW-PO-01-B

© 2007 Secure Computing Corporation. All Rights Reserved. WW-PO-Jan07vF. Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, SoftKhan, 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, IronIM, SecureWire, SnapGear, TrustedSource, On-Box, Securing connections between people, applications, and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.

## Today's business challenge: Protect. Enforce. Comply.

Organizations can do more over the Web today than ever before. As use of the Web continues to grow, virus outbreaks and other forms of Web-borne threats known as "malware" continue to grow as well. Are you adequately protected? Current security solutions such as IDS, traditional firewall, or anti-virus (A/V), while providing vital security, were not designed to combat malicious software code or cleverly blended threats, hidden inside seemingly good HTTP or HTTPS traffic, and targeted at individual organizations. While organizations need the Web, they need to be protected from attacks targeted at them.

## The Web Gateway Security Solution – Webwasher

Webwasher® adds an urgently needed layer of gateway security for today's Web environment which includes both inbound and outbound threats. Webwasher Web Gateway Security provides immediate protection against threats such as malware hidden in blended content, hidden in encrypted SSL traffic, and hidden in email. This in-depth security also protects organizations from outbound threats such as potential loss of confidential information that can leak out on all key Web protocols (HTTP, HTTPS, FTP, IM, and P2P).

## Five ways Webwasher can help your company

- 1. Best gateway protection in the business** – Webwasher Anti-Malware with ProActive security provides immediate protection for both Web and email traffic. It protects against spyware, day-zero, blended threats, and targeted attacks not available with traditional firewall or anti-virus solutions that solely rely on signature updates or heuristics. Webwasher combines this level of protection against *unknown malware* with the exceptional performance of a signature-based anti-malware engine for *known malware* threats to provide the industry's best Web Gateway defense against malware\*.
 

\* according to eWeek article "The Limits of Scanning" [http://www.securecomputing.com/pdf/246693\\_final.pdf](http://www.securecomputing.com/pdf/246693_final.pdf) (October 2, 2006)
- 2. Protection for encrypted traffic** – Webwasher is the first security product available with fully integrated SSL inspection. 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.
- 3. Added security through TrustedSource** – Webwasher is now integrated to the global TrustedSource™ reputation network to proactively find, report, and block traffic to and from questionable sources. Relying on its global reputation network and knowledge of Internet entities, the TrustedSource network identifies potentially malicious behavior or intentions to prevent malicious code from being distributed. For details, see the TrustedSource whitepaper ([http://www.ciphertrust.com/files/forms/landing\\_template.php?sp=CT\\_WhitepaperRequestForm&cr=trustedsource\\_web](http://www.ciphertrust.com/files/forms/landing_template.php?sp=CT_WhitepaperRequestForm&cr=trustedsource_web))
- 4. High performance proxy** – Webwasher is an enterprise strong proxy for HTTP, HTTPS, FTP, and SMTP traffic. Flexible authentication and routing features as well as built-in clustering support and availability on an ultra secure appliance make Webwasher an ideal choice for perimeter protection.
- 5. Inbound and outbound defenses**– Webwasher is unique in that it offers best-of-breed security solutions for incoming, blended threats such as worms, spyware, and malware on active Web pages, as well as tight control over data leakage.

“Some AV companies seem to have serious problems with the flood of malware users are receiving each day...”

Andreas Marx,  
AV-Test.org

## Comprehensive security

Webwasher’s arsenal of threat protection filters is designed to safeguard your network from targeted attacks launched by cyber criminals looking to profit from attacking your Web infrastructure. Webwasher Web Security Gateway uses multiple detection engines to make sure your network is protected:

- **Connection control layer:** The SmartFilter URL Filter module, powered by TrustedSource reputation technology, blocks secret “phone home” calls to spyware sites, access to Web sites distributing malware from infected machines and downloads of restricted executables. Webwasher Anti-Spam using TrustedSource connection control technology blocks unwanted email messages that often contain infected attachments or links to inappropriate or infected Web sites.
- **Media type blocking:** A powerful media type filter reliably detects the true file type and safeguards against files that are disguised to circumvent existing policies or security filters. Corporations may want to disallow media types that are potentially hazardous (like unknown ActiveX), bandwidth intensive, or a drain on productivity, such as video streams.
- **Anti-Malware Engine:** The Secure Anti-Malware Engine provides ultra-fast inspection of incoming and outgoing traffic for known signatures of viruses, spyware, bots, or other potentially unwanted programs.
- **Authenticode filter:** All active code is examined for digital signatures in the authenticode filter. Webwasher blocks active code based on the issuer or signature validity. This is a powerful way to keep unwanted active code out of a network but still allow regular maintenance updates or executables from known and well trusted sources.
- **Proactive Scanning:** Webwasher analyzes incoming traffic with active code to determine if it will behave in a harmless manner. If the behavior is not what is expected or is suspicious, the code is blocked. This behavioral malware detection is already deployed to more than 5 million customer seats worldwide. Whenever Proactive Scanning detects suspicious code, it is optionally submitted to Secure Computing’s TrustedSource reputation system.

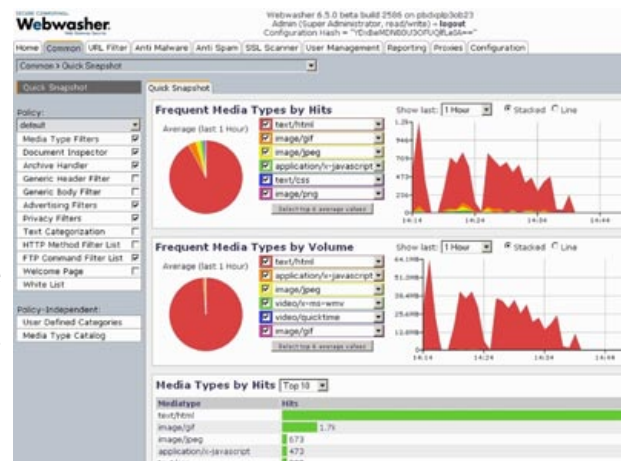


Figure 1: Webwasher security dashboard

## Webwasher solutions to protect your organization

Whether you need to protect your network from spyware, prevent employee access to restricted 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.

### Webwasher URL Filter

Reputation-based URL filtering prevents employees from accessing malicious, content and having it enter your network. The Webwasher URL filter powered by TrustedSource and the SmartFilter Internet database, significantly reduces productivity losses, legal risks, and security exposure caused by unauthorized employee access to inappropriate, malicious or distracting Web content. Additionally, URL Filter significantly reduces bandwidth consumption by blocking unwanted content like advertising and pop-ups. Webwasher URL Filter comes with an easy-to-use drill-down reporting solution so you always know where your employees spend their time when surfing the Web.

## Webwasher Anti-Malware

Webwasher Anti-Malware is the best available solution to block known and unknown or hidden malware like viruses, spyware, key-loggers for Web and email even if they are downloaded within an encrypted SSL session. Organizations are now targeted by malicious attacks focused solely on them and signature-based anti-virus (A/V) vendors do not provide defenses against these attacks. Webwasher combines the exceptional performance of a signature-based anti-virus and anti-malware engine for known malware with the ruggedness of our ProActive Security filters to detect blended or yet unknown bad content. Deep content inspection makes sure that malware is reliably detected even if hidden deep in compressed or spoofed files.

## Webwasher Anti-Virus

Webwasher Anti-Virus provides a robust and enterprise strong® gateway against viruses and malicious code in Web, FTP, and mail traffic. Its unique combination of multiple third-party signature-based anti-virus engines allows the deployment of multiple anti-virus solutions at the same time without the usual hits in performance and latency. Customers who wish to deploy industry leading engines at the gateway will find their needs served by Webwasher Anti-Virus.

## Webwasher Anti-Spam

Anti-spam represents the first line of defense against malicious code entering through the gateway via email. Secure Computing research shows nearly all emails with executable attachments that are classified as spam are infected with some form of malware. Webwasher Anti-Spam also protects against Phishing attacks and the nuisance of unwanted mails.

## 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 providing scanning of SSL (HTTPS) traffic, which most vendors cannot provide, Webwasher enables enterprises to apply their existing security and Internet usage policies to all key Web protocols.

## Webwasher Content Reporter

Content Reporter provides an in-depth view of the peaks, trends, and events relating to all network activity, including cache, streaming media, Web, and email usage. Highly scalable and with automated collected data from multiple sources, it is an excellent reporting solution for global corporations.



"The No. 1 product, Webwasher by Secure Computing, detected 99.97% out of the 289,682 samples."

The Limits of Scanning, eWeek, October 2, 2006

[http://www.securecomputing.com/pdf/246693\\_final.pdf](http://www.securecomputing.com/pdf/246693_final.pdf)

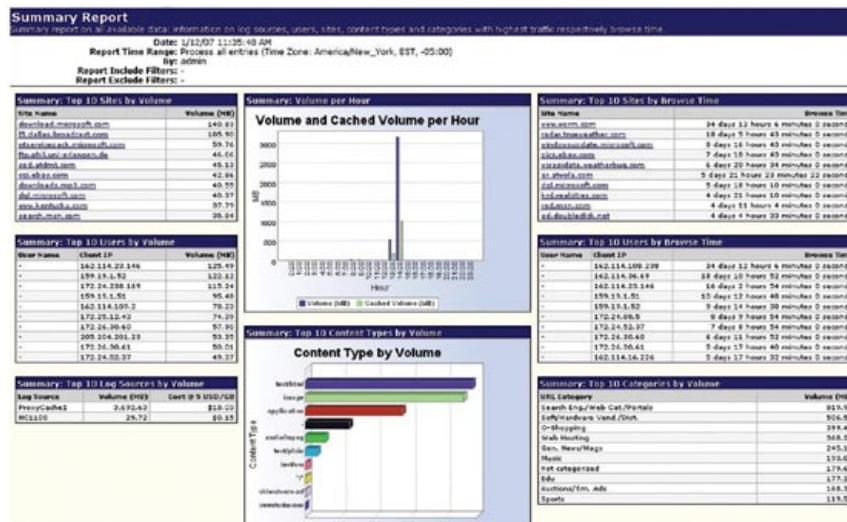


Figure 2: Comprehensive reporting on Web traffic



### 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](mailto:sales@securecomputing.com)  
[www.webwasher.com](http://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](http://www.securecomputing.com/goto/globaloffices)

## Key benefits Webwasher appliances

Webwasher is available as high-performance appliances for every budget and performance demand as well as software for Linux, Solaris, and Windows platforms.

### Hardened against attacks

Webwasher appliances benefit from the same hardened operating system as our firewalls, preventing attacks against the security gateway itself. Secure Computing's firewall appliances have a track record of *zero compromises*.

### Easy to install and deploy

Webwasher appliances come completely preinstalled and 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 always up-to-date anti-malware, anti-spam, and URL data. An update mechanism allows remote network-based updates and maintenance of the appliance.

- **Fully integrated** – Webwasher completely integrates and includes multiple protections that would otherwise require multiple stand-alone products, such as URL filter, anti-virus, anti-spam, anti-spyware, SSL Scanner, and content control filters in one single and easy to manage solution. This leads to significant savings in terms of management, deployment, and handling/purchasing.
- **Multiple filtering engines** – Unlike solutions that rely only on signature updates to provide protection, Webwasher uses a combination of several filters to stop threats. Webwasher's Proactive Security filters provide immediate protection by detecting blended or yet unknown malware. Its fast signature-based anti-virus and anti-malware engines detect known viruses and other potentially unwanted programs, many of which turn out to be spyware or adware-related programs such as keystroke loggers. Webwasher's use of multiple filters provides the industry's best Web Gateway security\*.
- **High-Performance** – Anti-Virus PreScan™ filtering technology radically improves performance by reducing the load sent to the anti-virus engine.
- **Flexible deployment** – Webwasher uses the industry standard ICAP (Internet Content Adaptation Protocol) to efficiently communicate with other security appliances, as well as an array of industry standard proxy/caching devices, plugins for Squid, ISA Server, proxy chaining and the IFP protocol.
- **Single point of administration** – Because all Webwasher modules are tightly integrated, Webwasher's efficient policy management enables administrators to specify policies once that apply to all products and are valid for all Web, SSL, and FTP traffic.
- **Comprehensive content filters** – The efficiency of the security filters is augmented with an array of additional filters that provide rule-based protection against all types of Web and email-borne threats. The built-in archive handlers open .zip, .gzip, .tar, .arj, and other archives for content scanning. The built-in "Document Inspector" scans Word, XML Excel, PowerPoint, and PDF documents recursively for unwanted content and malicious code.



Model name	WW 500	WW 1100	WW 1900
Form factor	1U rack mount	1U rack mount	1U rack mount
RAM	1 GB	1 GB	2 GB
Processor	Single	Dual core	2 Dual core
Processor cache	1 MB	2 x 2 MB	2 x 2 MB
Disk	80 GB SATA	2 x 80 GB SATA	2 x 146 GB SAS
RAID	–	Raid 1	Raid 1
Power supply	single	single	redundant
Interfaces	2 x 10/100/1000	4 x 10/100/1000	4 x 10/100/1000
Suggested users*	4,000 - 10,000*	8,000 - 20,000*	16,000 - 40,000*

\* higher number denotes URL filtering only