

www.securecomputing.com

Secure Computing^{fi} has been solving the most difficult network and application security challenges for over 20 years, and is uniquely qualified to be the global security solutions provider to organizations of all sizes.



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

eWeek anti-malware report, performed by AV-Test.org

According to an independent test comparing the detection rates of 27 anti-virus and anti-malware products, Webwasher Anti-Malware provides the industry's best* security against spyware, day-zero, and blended threats not available with traditional anti-virus protections or stateful inspection firewalls.

*according to eWeek
The Limits of Scanning
http://www.securecomputing.com/pdf/246693_nal.pdf
(October 2, 2006)

© November 2006 Secure Computing Corporation. All Rights Reserved.
WWW-AntiMail-PO-NextView- Boss, enterprise strong, IronMail, MobilePass, PremierAccess, SafeView, Secure Computing, SecureOS, SecureSupport, Sidewinder, G2, SmartFilter, SoftToken, Sinkback, Type Enforcement, CyberGuard, and Webwasher are trademarks of Secure Computing Corporation, registered in the U.S., Patent and Trademark Office and in other countries. Anti-Virus Multi-Scan, Anti-Virus PreScan, Application Defenses, Compliance, Dynamic Quarantine, Edge, Encryption, G2, Enterprise Manager, Global Command Center, IronMail, IronMail, Live Reporting, Message Profiler, Methodville, On-Box, Outbreak Defender, PowerHunt, Radar, RemoteAccess, Secure Encryption, SecureWire, SmartReporter, SnapGear, SpamProfiler, Threat Response, Total Stream Protection, TrustedSource, TrustedSource Portal, WebMail Protection, and ZAP are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.

Webwasher Anti-Malware

Today's business challenge

Organizations need protection from viruses and malware entering their networks as well as safeguard mechanisms to keep confidential information from exiting their corporate network. Current protection systems, such as stateful firewalls or gateway anti-virus protection alone are not designed to combat today's threats which are targeted at specific enterprises and cleverly hidden inside seemingly good HTTP or HTTPS traffic. Furthermore, targeted malware attacks by criminals against organizations may be limited enough in scope as to not garner the attention of traditional reactive signature-based anti-virus vendors. According to the 2006 CSI/FBI Computer and Crime survey, 97% of the enterprises surveyed use an anti-virus software and 98% use a firewall of some kind; nevertheless almost two thirds (65%) suffered a malware outbreak or incident.

The solution: Webwasher Anti-Malware

Webwasher^{fi} Anti-Malware from Secure Computing^{fi} immediately protects your organization's networks from known, unknown, and small-scale targeted attacks (in terms of scope, but could be large-scale in damages to an organization), including viruses, Trojans, spyware, and the loss of confidential information. Webwasher Anti-Malware protects all Web and email traffic, including encrypted HTTPS traffic, if used with the Webwasher SSL Scanner module.

Unlike traditional anti-virus engines that rely *only* on signatures, Secure Anti-Malware uses a combination of several proactive filters to stop threats. Webwasher's Proactive Security Filters detect blended or yet unknown malware, while its signature-based anti-malware engine is used to detect known threats*.

Key benefits

Proactive Filter technology Provides immediate protection by blocking unknown malicious code, day-zero attacks, and exploits already at the gateway and neutralizes suspicious script code. This is critical for organizations targeted by small-scale malicious attacks that would not garner the attention of traditional anti-virus vendors.

Signature-based blocking - Webwasher Anti-Malware provides fast signature-based blocking of known viruses and other potentially unwanted applications/programs, many of which turn out to be spyware or adware-related programs such as keystroke loggers.

Comprehensive content filters - The efficiency of the security filters is augmented with an array of filters that provide rule-based filtering protection against all types of Web and email-borne threats.

Archive Handler for .zip, .gzip, .tar, .arj, and other archives.

Document Inspector scans Word, XML Excel, Powerpoint, and PDF documents recursively for unwanted content.

Embedded Objects Filter scans for objects embedded in other files and Web pages.

Macro Filter for potentially harmful macros in Microsoft[®] Office documents.

ActiveX, media-type, and upload filters.

Advertising, privacy, and cookie filter.

High-Performance Anti-virus PreScan filtering technology radically improves performance by reducing the load sent to the anti-virus engine.

Easy to manage - Webwasher allows unlimited and flexible policies that are specifically tailored to your organization's unique structure and requirements.

Full proxy Webwasher is an *enterprise strong*^{fi} 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.

ICAP support - Webwasher uses the industry-standard ICAP (Internet Content Adaptation Protocol) to communicate efficiently with other security appliances, as well as an array of industry-standard proxy/caching devices.

