

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

Catching Spies with Secure Web (Webwasher) Solutions

(Secure Web Anti-Spyware/Anti-Malware Tactics)

Table of Contents

Overview	2
Shaken, Not Stirred	2
Evil Geniuses at Work	2
Secure Web (Webwasher) Eliminates Spyware on All Fronts	3

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 +44.0.1344.312.600

Asia/Pac 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

Overview

Do you think that nobody would be interested in spying on your network? Think again. Spyware has become a major threat to enterprise network security, and according to IDC, 67 percent of all computers have some form of spyware.

If you run the nation's Defense network, protect the Colonel's secret recipe, or are the guardian of the Internet's "Next Big Thing," it's likely that you're worried about spies, and you would be right to be paranoid. But spyware isn't just about stealing the big secrets of the world, it's all about the little things. Spyware pilfers your passwords. It's a kleptomaniac of keystrokes; it's a shady salesman with a loud tie lurking inside your computer waiting to see where you've surfed.

And just like a good spy with a briefcase full of fake moustaches, spyware takes many forms.

Shaken, Not Stirred...

Think of Secure Computing's Secure Web (*Webwasher*) portfolio as the James Bond of Internet security. Bond has a scientist that provides him with all sorts of goodies—fast cars that sprout wings and shoot flames out the back, ultra-sensitive listening devices, and special glasses that can see through walls. He has a tool ready for any eventuality.

So too with our Secure Web solution. Preventing spyware can't be done with a single piece of software or filter. Secure Web packs multiple Web security solutions in a single appliance, so multiple avenues are closed off to spyware.

1. **Secure Web Filter** prevents employees from surfing to sites that are known to harbor spyware and other malicious software.
2. **Secure Web Anti-Malware** provides immediate protection against threats such as spyware, Trojans, and other malware hidden in Web pages. Secure Web Anti-Malware accomplishes this by analyzing the nature and intent of all content and active code entering the network via Web pages. (For third-party confirmation of Secure Web's malware catch rates.
3. **Secure Web Anti-Virus** provides unique Anti-Virus Multi-Scan technology that combines the strength of multiple anti-virus engines concurrently scanning all Web traffic.
4. The **Secure SSL Scanner** makes sure that spyware isn't hiding in SSL-encrypted traffic.
5. **Secure Web IM** detects, reports, and selectively blocks the unauthorized use of high-risk Peer-to-Peer file sharing (P2P) and Public Instant Messaging (IM) from your network.
6. **Secure Web Cache** offers a revolutionary new design that employs proactive scanning and security reputation prior to delivering a cached object to an end-user.
7. **Secure Web Content Reporter** provides an in-depth view of the peaks, trends, and events relating to all network activity, including cache, streaming media, and Web usage.
8. Furthermore, Secure Web includes **TrustedSource™** technology reputation-based filtering to round up all the usual suspects—accurately predicting the reputation of every URL, and IP before deciding whether or not to allow them into the network.

Evil Geniuses at Work

The Web has become more powerful than we ever imagined. Web 2.0 applications continue to evolve and make it easier for us to connect, share information, and do business in an online virtual environment. Some applications are already claiming "Web 2.5" status, and visionaries are starting to put together what "Web 3.0" will look like.

At the same time, cyber-attackers are also taking their own technology up many notches. They may hide malware inside of encrypted SSL traffic. More often than not, an attack will target multiple vectors to increase the chances of breaking in. Disseminators of spyware have several different ways they penetrate your computer. These include:

- **Trojans.** Have your employees downloaded applications on their computers that weren't authorized? They seem harmless, and take the form of cute wallpaper or screen savers, games, or small utility programs. But buried inside these little gems is a dangerous payload, secretly funneling information out of your network.
- **Active Code.** When you walk past an employee, are they looking guilty as they quickly exit their browser and replace it with a spreadsheet? Counter-productive Web surfing can cause legal liabilities, offend others in the office, and cause bandwidth problems, but most of all, it can result in spyware. Pornographic Web sites and gaming sites are notorious for secretly hosting spyware. Your employee may believe they are playing a harmless online game, but there's a very good chance that they've already allowed spyware into their computer without knowing it.
- **Email phishing.** Almost everybody within the enterprise has email access, and this is the way it should be. But there are dangers there too, and the spam emails that come through will get opened and read. Many such spam emails are obviously bogus and make outrageous claims—but the more skilled spammers will send out emails that claim the recipient has received an e-card, or attempt to mimic an email from a legitimate source. The email contains a link, which the recipient clicks on—and then becomes infected with spyware.
- **IM/P2P.** Instant messaging and peer-to-peer applications, when used in a controlled environment, bring tremendous benefit to users. However, when employees load unauthorized IM or P2P clients onto their computers, spyware often is the result.

Secure Web (*Webwasher*) Eliminates Spyware

There are a number of "anti-spyware" tools available, but most of them are single point-products that neglect some of the more sophisticated ways that attackers use to send spyware to your network. Simply deploying a signature-based anti-spyware tool for example, may prevent some spyware from getting into the network, but not all of it. Spyware hidden in encrypted traffic, and new "zero-day" spyware threats that have not yet been included in signature databases, will still get in. The Secure Web strategy goes far beyond those single point solutions, and closes off every possible avenue for spyware.

Secure Web (*Webwasher*) is the best there is at blocking malware—#1 rating of 99.83%

The Secure Web protection strategy leaves behind a long trail of thwarted spyware attempts. In a test run by AV-Test, an independent research facility at the Otto-von-Guericke University in Magdeburg, Germany, 29 anti-malware products were tested against a set of 606,901 files. **The test included 407,487 Trojan horses, 82,659 worms, 68,864 backdoors, and 47,891 bots. Out of the 29 products tested, Secure Computing's Webwasher scored highest with a 99.83 percent detection rate**—significantly above the average score of 86.95 percent. Products were scored on several different criteria. In addition to taking into account the scanning percentage, the rank also considered number of false positives, proactive detection, and response times to new malware. Although Secure Web scored well on all counts, its high score in proactive detection sets it apart from the others. This category ranked how well products did in detecting threats that had no signature.

For more information these test results, please see this article (<http://www.securecomputing.com/index.cfm?sk=1804#webwasher>)

Secure Web (*Webwasher*) accomplishes its anti-spyware feats by:

- Preventing the installation of spyware
- Detecting existing spyware when it attempts to upload potentially private data or contact its home base
- Blocking downloads of Windows executables via the Web by unknown Web browsers or adware/spyware clients

- Blocking Web sites that are known to, or are likely to have, spyware
- Locking out client computers with spyware installed
- Accurately determining the reputation of all URLs and IP addresses

The Secure Web arsenal includes both inbound and outbound defenses, which adds an extra layer of protection against spyware. Inbound defenses prevent spyware from entering the network in the first place, and the outbound defenses add an extra layer of protection. In the unlikely event that spyware does enter the network, or there is already existing spyware, Secure Web's outbound protection will know if a piece of spyware is trying to send information back to its host—and will stop it before your data can leak out.

For more information about Secure Web and our other enterprise security solutions (Secure Mail, Secure Firewall, and Secure SafeWord), please visit Secure Computing at <http://www.securecomputing.com>.