

# Dealing With Adware And Spyware

Lisa Phifer

**You'll need a hybrid of host- and network-based approaches, as well as the security professional's greatest asset: Constant vigilance.**

If early viruses like BubbleBoy and LoveBug make you pine for simpler times, then you are probably waging war against this millennium's far more tenacious foe: The stubborn crop of spyware that now infests three out of four PCs. From pesky adware like BonziBuddy to malicious malware like Trojan-Downloader-Zlob, spyware is literally choking corporate desktops and networks. Responsible for one out of four help desk calls and half of the PC crashes reported to Microsoft, spyware is draining IT resources and business productivity.

Worse, spyware is now morphing from nuisance to nightmare. Those seeking financial gain through spyware have evolved from tracking cookies and intrusive pop-up ads to more selective and insidious methods. For example, drive-by-downloads are installing exploit code onto PCs that merely visit websites, without user interaction. Phishing trojans are monitoring browser activity, waiting to capture identities and credentials during on-line banking transactions. Keyloggers are harvesting sensitive data from victims, violating privacy laws and industry regulations.

## Stamping Out Spyware

Associated business risks are making it impossible for companies to ignore spyware. The Radicati Group projects that anti-spyware spending will grow from \$103 million in 2005 to more than \$1 billion by 2009. Many companies can justify invest-

ment just by reducing spyware remediation cost. Webroot estimates that help desk calls, resurrecting compromised workstations and the resulting down time run about \$250 per user, per year (a calculation is shown in Figure 1).

Potential return on investment does not end there. Spyware not only slows desktops; it saps worker productivity and hogs bandwidth. According to SurfControl, ISPs find that peer-to-peer spyware programs (e.g., Grokster, KaZaA, Limewire) generate up to 70 percent of network traffic. Spyware that exposes private data may result in embarrassing public disclosure, costly customer notification and compliance violations that bring hefty fines. Spyware is also a popular vector for executing electronic crimes like identity theft and on-line fraud. In one well-publicized case, 22 Israelis were arrested for using spyware to commit corporate espionage. While data theft costs are notoriously difficult to quantify, the gravity of such incidents cannot be denied. Business consequences are already significant, and will continue to escalate as spyware grows more virulent.

Unfortunately, defeating spyware is harder than evading conventional viruses. Spyware is any potentially-unwanted program that makes undesirable changes to your computer and/or collects information about user activities, without consent, usually for financial gain. That definition may be fine in the abstract, but making concrete decisions

*Lisa Phifer is an owner and principal consultant at Core Competence, a network security technology consulting firm based in Chester Springs, PA. A 25-year veteran of the networking industry, Lisa has been battling the spyware scourge since 2001. She can be reached at [lisa@corecom.com](mailto:lisa@corecom.com).*

**FIGURE 1 Cost Of Spyware (A Calculator)**

Number of Workstations:	<input type="text" value="1000"/>
Average Hours to Re-image:	<input type="text" value="6"/>
Hourly Value of Employee Time:	\$ <input type="text" value="40"/>
Re-image Rate:	<input type="text" value="2"/>
Average Cost per Help Desk Call:	\$ <input type="text" value="15"/>
Monthly % Chance of Spyware Call:	<input type="text" value="10"/> %
<b>Total Cost of Spyware:</b>	<b>\$248,400</b>

Source: Webroot

about which programs are really spyware can be difficult.

■ **Annoying Adware**—Many programs monitor activity, but when does that become a breach of privacy? Cookies retain personal information—usernames, passwords, preferences—so that websites can improve user experience. But some cookies share tracking data with third parties that deliver pop-ups and banner ads; those installed without user consent are called adware cookies. And then there are programs like WeatherBug and Surf-SideKick that display sponsor ads while they run. Such adware programs may or may not obtain consent to track and share personal data through end user license agreements—which most users simply accept without reading.

■ **Nebulous NonBizWare**—Many workers install non-business software on corporate PCs, from IM and softphones to multi-user games and peer-to-peer file sharing. Beyond reducing productivity, NonBizWare establishes communication “back channels” that could be exploited to penetrate or attack a corporate network.

NonBizWare may also expose employers to legal liability associated with distribution of copyrighted music, pirated software and pornographic material. Therefore, even though NonBizWare may not “spy” on users, many anti-spyware solutions treat these potentially-unwanted programs as another form of spyware.

■ **Menacing Malware**—A growing percentage of spyware is malicious software intended to damage a computer, steal data, or create an attack platform. For example, browser hijackers like CoolWebSearch\_xplugin change home pages, redirect Web searches, and misdirect URLs to phishing pages and pay-to-play search engines. Keyloggers like SpyBuddy record document edits, email, instant messages, chat room conversations and Web form responses by relaying user keystrokes to remote attackers. Botnets use worms or trojans to plant drones like SoberQ that listen for IRC commands instructing them to relay spam or join DDoS attacks. Trojan downloaders like Zlob and Wstart hide in attachments and downloads, opening back doors through which other programs can be remotely installed. Rootkits like NTRootKit are trojans that operate as hidden system files, letting attackers gain unrestricted access to a “rooted” computer. And the list goes on.

Unlike adware and NonBizWare, there is little room for interpretation here: Malware rarely belongs on any system.

■ **Rogue Anti-Spyware**—Finally, spyware itself has created an opportunity for rogue anti-spyware—programs like SpyAxe, Winhound, and SpyTrooper that use pop-up ads and scare tactics to convince users to download phony anti-spyware programs. When executed, many of these rogues generate “false positive” warnings that hound users into purchasing clean-up programs or paid feature licenses.

These are but a few of thousands of pieces of code congregating under the spyware umbrella. They illustrate that spyware is extremely diverse in delivery method, installed behavior and potential impact. These characteristics make spyware challenging to detect, and even more challenging to mitigate. In short, spyware is a complex threat that is most effectively addressed through multi-phase, multi-layered defenses.

#### **Phase One: Proactive Prevention**

The old adage, “An ounce of prevention is worth a pound of cure” certainly applies to spyware. Once spyware has been installed on a host, it can be extremely difficult to return that host to a trustworthy state. Efficient spyware defense starts with proactive steps intended to circumvent popular delivery methods.

Spyware has a penchant for social engineering—from tricking users into clicking on fake pop-ups to bundling trojans with enticing shareware. We cannot depend on users to “do the right thing,” but we can still benefit from spyware education. Many on-line resources exist, including StopBadWare.org, StaySafeOnline.org, CERT Cyber Security Tip ST04-016, and knowledge bases published by reputable anti-spyware vendors. But take care to avoid rogue anti-spyware—see [www.spywarewarrior.com/rogue\\_anti-spyware.htm](http://www.spywarewarrior.com/rogue_anti-spyware.htm).

Spyware often makes its way onto a desktop through a Web browser. Secure browser configuration can help to stop hijackers and drive-by downloads. ActiveX controls are a spyware favorite; disabling unsigned ActiveX is a simple but valuable step. Disabling Java applets can also be helpful, but more likely to cripple legitimate websites. These and other browser configuration tips can be found online, including <http://cybercoyote.org/security/browsers.shtml>. Companies should disable user prompting, enforcing active content and plug-in settings with a desktop management tool like Active Directory Group Policy Objects.

Many adware cookies and browser hijackers can be neutralized by configuring browser Privacy settings to disable third-party cookies and block pop-ups. Exceptions can be made for legitimate websites that require these features to operate correctly, preferably by importing a company-defined list of permitted sites. Pop-up blockers are freely available from many sources, including the Windows XP SP2 upgrade for Internet Explorer and the Google Toolbar.

Use Internet Explorer’s Restricted Site Zone (or equivalent features in other browsers) to block access to known adware and spyware sites. But do not attempt to populate this list manually. Instead, use a tool like JavaCool SpywareBlaster to configure this banned site list, and update that list regularly as new sites emerge.

Many spyware programs need administrative



## **Spyware has a penchant for social engineering**

**It is necessary to combine prevention with detection**

rights to install themselves, overwrite OS files or disable security measures in an effort to evade detection. Those threats can be crippled or neutralized by browsing the Web from a Least-Privileged User Account (LUA). Never browse the Web as administrator. If you must, use a free tool like Microsoft DropMyRights to downgrade privileges when launching your browser (or any other Internet application).

A significant percentage of spyware has been designed specifically to exploit Internet Explorer features or vulnerabilities. Diligent patching can make a big difference, as can upgrading to a newer version of IE. Security improvements found in IE version 7 include ActiveX opt-in, a “No Add Ons” mode, a “Fix My Settings” option, and better protection from cross-domain scripting attacks. Or consider using an alternative browser like Firefox for general Web surfing, reserving IE for known/trusted sites that do not work well otherwise. Alternative browsers may be a less popular spyware target, but they still require secure configuration and patching.

Browsers may be spyware’s favorite target, but many other applications can fall victim. For example, email can carry spyware in file attachments,

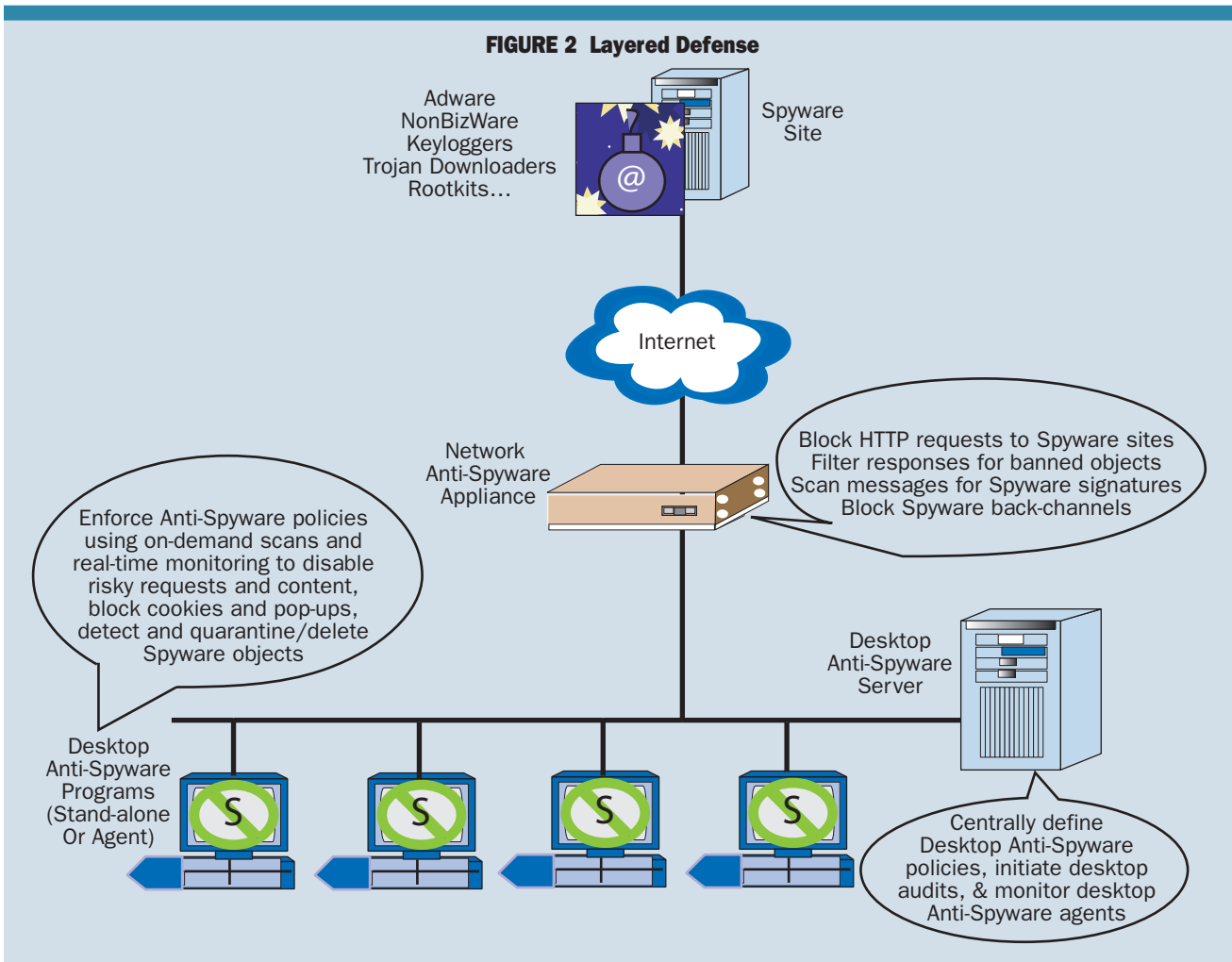
or contain embedded URLs for spyware websites. This risk can be reduced by using non-IE viewers when displaying HTML content, using application settings to disable active content and script execution, stripping risky file attachments, and flagging deceptive URLs. Spam filtering can also weed out many dangerous messages before users have an opportunity to get themselves in trouble when reading them.

Finally, spyware and adware do their dirty work by communicating with third parties. Preventing back-channel communication literally renders these programs mute. DNS black holes can be used to resolve host names and domain names that are known to propagate spyware to the loopback address 127.0.0.1. Entries can be added to desktop HOSTS files, DNS Servers, or both, using lists maintained by the Bleeding Snort DNS Black Hole project.

**Phase Two: In-Depth Detection**

These proactive steps, coupled with persistent patching, list maintenance, and configuration enforcement, can significantly reduce spyware. But prevention is never foolproof. Spyware sites move, users add exceptions, and NonBizWare

**FIGURE 2 Layered Defense**



sneaks in on thumb drives. It is therefore sensible to combine prevention with detection.

Spyware may be harder to classify and eradicate than conventional viruses, but anti-spyware defenses can be deployed in network locations similar to those used for anti-virus: on the desktop, at the network edge, and as a managed service (Figure 2).

■ **Desktop Anti-Spyware**—Many host-resident anti-spyware programs are available as consumer packages or enterprise solutions. Features vary, but most provide start-up scans, on-demand scans, and real-time memory/file/application monitors. On-demand scans can provide periodic audits, but real-time monitoring is essential to avoid complicated cleanup. Fortunately, anti-spyware has evolved from spotting consequences to quarantining spyware before damage is done.

Anti-spyware programs have long detected potentially-unwanted changes to cookies, registry keys, hosts files, browser zones and running services—signs that spyware is being installed. Some anti-spyware programs can block activities that presage spyware installation, like suspicious ActiveX execution and browser helper object installation. Most anti-spyware programs use signatures to compare Web and other application objects to thousands of known culprits, preventing installation of NonBizWare, hacker tools, keyloggers, trojans and worms. To keep up with new spyware that morphs, behavior-based detection is being added to some anti-spyware programs. And to detect evasive threats like rootkits, anti-spyware programs have also started to monitor activity with lower-level drivers.

Anti-spyware options like scan location/depth and exclusions can be helpful—for example, ignoring an IM client used for business or your own website's adware cookies. Most anti-spyware programs keep a local log of detection results, with hot links to spyware definitions, ratings and advice. However, anti-spyware programs may or may not provide automated spyware removal (see the section on "Remediation").

Some consumer anti-spyware programs provide free scanning, but require a paid license to activate advanced features. Because spyware detection varies, running more than one program can be useful, and combining a paid program with free tools is common. Freely-available consumer anti-spyware programs are available from many sources, including Microsoft Windows Defender, SpyBot-S&D and WinPatrol.

Why spring for a commercial desktop anti-spyware program? Vendors that offer both free and commercial anti-spyware tend to reserve the most valuable features—notably real-time monitoring and automated removal—for paid customers. Moreover, SMBs and enterprises require features that are absent in consumer anti-spyware programs:

Businesses should look for centralized policy

definition, including the ability to customize scan depth, permitted exclusions, prohibited Non-BizWare, quarantine/delete actions, signature updates and audit schedules. Larger enterprises may prefer group-based policies that can apply different lists and schedules to regular users, administrators and high-value systems.

Enforce centrally-managed policies with configuration locks, preventing users from adding their own exceptions or disabling spyware protection. However, some exceptions may be necessary for employees to do their jobs. For best results, choose a policy engine that lets you selectively permit end user changes, but disable end user prompting except where required to meet business needs.


Businesses may also need real-time monitoring and historical reporting features that let administrators identify where and when spyware has been encountered, and steps that were taken to automatically remediate it. Look for threat assessment aids, like the ability to single out un-remediated hosts and filter by spyware type/severity.

Larger enterprises should also consider scalability, including server/database platform requirements, hierarchical/group views, update distribution, integration with enterprise desktop and network management systems and cost per desktop.

Enterprise anti-spyware solutions available today include Computer Associates eTrust Pest Patrol, eSoft Desktop Anti-Spyware, Futuresoft DynaComm i:scan, Lavasoft Ad-Aware Enterprise, McAfee Anti-Spyware Enterprise, Shavlik NetChk Spyware, Sunbelt CounterSpy Enterprise, SurfControl Enterprise Threat Shield, Tenebril Spy Catcher Enterprise, Trend Micro Anti-Spyware Enterprise and Webroot Spy Sweeper Enterprise.


■ **Network Anti-Spyware**—A healthy crop of anti-spyware appliances has emerged to complement desktop anti-spyware. Stopping spyware at network trust boundaries avoids over-dependence on desktop defenses. Network appliances let you uniformly enforce anti-spyware policies on all users, including contractors and visitors. When a new threat emerges, or you decide to permit business use of a P2P program, anti-spyware appliances can apply the modified policy immediately. Appliances provide a single point for spyware quarantine, reducing the risk of desktop infection and costly clean-up. Finally, anti-spyware appliances are less likely to fall victim to spyware, like malware that tries to disable desktop security programs.

However, network anti-spyware is no panacea. As with any perimeter defense, anti-spyware appliances cannot stop installation of spyware that originates inside the network (e.g., NonBizWare installed from USB stick). Network-based solutions must balance security and performance to avoid becoming bottlenecks. They may not excel at making per-user exceptions or desktop



## Network-based solutions allow for more uniform enforcement





## Malicious spyware removal is not for the faint of heart

remediation. Finally, network anti-spyware cannot protect laptop users when they work (and surf the Web) remotely.

Combining desktop and network anti-spyware creates a layered defense that is more robust and resilient than either would be alone. In fact, some vendors offer both solutions, leveraging common components like management tools and signature databases.

What functions can you expect from an anti-spyware appliance?

- A network appliance is a convenient place to filter outbound HTTP requests, blocking installer downloads, known spyware URLs, and black-listed domains.

- A network appliance can also strip active content from HTTP responses, including ActiveX controls, Java applets, scripts and banned S/MIME types.

- After filters are enforced, an appliance may use signatures to scan inbound application payloads, quarantining suspicious data objects.

- A network appliance may also block adware and spyware back channels, including P2P protocols like ICQ and malware that sneaks out on port 80.

Some anti-spyware appliances operate as Web proxies with the ability to scan SSL-encrypted HTTP (e.g., Finjan Vital Security Web Appliance, Bluecoat SG). Some watch for standard protocol deviations, vulnerabilities and associated exploits (e.g., Aladdin eSafe Gateway). Some appliances focus on spyware (e.g., 8e6 R3000 Enterprise Internet Filter), while others combine anti-spyware with many other network defenses (e.g., eSoft Threatwall). Finally, many anti-spyware appliances operate as in-line gateways (e.g., FaceTime RTGuardian, McAfee Secure Web Gateway), but some offer out-of-band spyware detection (e.g., Mi5 Enterprise SpyGate).

- **Anti-Spyware Services**—Managed security services are generally aimed at those short on IT staff, security expertise, and capital. As spyware concerns grow, new managed anti-spyware services are expected to emerge for individuals and businesses.

Windows Live OneCare illustrates this trend at the desktop. OneCare Protection Plus is a subscription-based managed security service that combines desktop anti-spyware, anti-virus, and firewall defenses. OneCare primarily targets individual consumers, but can also be used by small businesses that prefer not to configure, monitor, or maintain desktop security programs. Other vendors have also announced subscription-based desktop security services that will include anti-spyware, notably McAfee Falcon and Symantec Norton 360 (aka Genesis).

At the network edge, providers that deliver CPE-based managed security services are adding anti-spyware. Many already wrap expert provisioning, 24/7 NOC monitoring, threat assessment

and incident response around multi-function security appliances from vendors like McAfee, Trend Micro, SonicWALL and WatchGuard. Providers can spin anti-spyware modules for these and other security appliances into new anti-spyware offerings, accompanied by professional services like spyware remediation.

### Phase Three: Rigorous Remediation

Spyware prevention and detection can reduce the need for remediation, but hosts that are already infested with spyware must be cleansed before applying prophylactic measures.

Relatively benign threats like adware cookies and NonBizWare programs can often be removed manually without difficulty. Temporary files, browser caches, cookies, and play-by-the-rules programs can be deleted with standard desktop tools like Disk Cleanup and Add/Remove Programs. Unfortunately, removing more tenacious adware, bots and trojans without crippling the host can be very tricky. Malware that morphs to elude detection can affect each host in a slightly different fashion. Rootkits are especially tough to scrub because they replace OS files and use hidden processes.

As a result, malicious spyware removal is not for the faint of heart. Vendor knowledge bases and public forums like CastleCops offer manual spyware removal advice, but most businesses should rely on automated clean-up using desktop anti-spyware programs. In addition to real-time quarantine, some anti-spyware products include rollback/restore capabilities that can recover critical files over-written by spyware. On Windows XP SP2 hosts, Microsoft's Malicious Software Removal Tool (MSRT) can be used to delete the most prevalent malware.

When spyware removal fails or produces questionable results, rebuilding the desktop can be required for recovery to a trustworthy state. For companies that already maintain standard desktop images and regular data backups, re-imaging may be time-consuming but tolerable. Others may find repeated spyware remediation costly enough to justify investment in the aforementioned practices, reaping benefits beyond spyware relief. Those without previously-saved desktop images may find themselves with little choice but to disconnect the infested host from the Internet, quickly back up critical data to CD, reformat hard disks, and reinstall the operating system and applications from scratch.

Alternatively, some experts recommend browsing the Web from virtual machines (e.g., VMware Workstation, Microsoft Virtual PC). This kind of "sandboxing" can insulate your real operating system, letting spyware damage be undone simply by discarding the compromised virtual machine. Those who routinely use virtual machines for other reasons (e.g., software development and testing) may find this approach very helpful.

## Conclusion

Fighting spyware may seem like an uphill battle, but it is a campaign that most of us have little choice but to wage. Over a 15-month period, Microsoft's MSRT alone removed 16 million instances of malicious software from 5.7 million computers, 62 percent of which housed at least one backdoor trojan. Even the most computer- and security-savvy Internet users occasionally fall victim to spyware. Given the financial gain that drives spyware, these pests will undoubtedly continue to proliferate. For spyware, the best defense is a strong offense: taking reasonable steps to prevent and detect spyware can reduce your risk of compromise and your need for expensive remediation□

### Companies Mentioned In This Article

8e6 Technologies ([www.8e6.com](http://www.8e6.com))  
Aladdin ([www.aladdin.com](http://www.aladdin.com))  
Bleeding Snort DNS Black Hole project  
([www.bleedingsnort.com/blackhole-dns/](http://www.bleedingsnort.com/blackhole-dns/))  
Blue Coat ([www.bluecoat.com](http://www.bluecoat.com))  
CastleCops ([wiki.castlecops.com/PIRT](http://wiki.castlecops.com/PIRT))  
CERT ([www.cert.org](http://www.cert.org))  
Computer Associates ([www.ca.com](http://www.ca.com))  
eSoft ([www.esoft.com](http://www.esoft.com))  
FaceTime ([www.facetime.com](http://www.facetime.com))  
Finjan ([www.finjan.com](http://www.finjan.com))  
Futuresoft ([www.futuresoft.com](http://www.futuresoft.com))  
Google ([www.google.com](http://www.google.com))  
Lavasoft ([www.lavasoft.com](http://www.lavasoft.com))  
McAfee ([www.mcafee.com](http://www.mcafee.com))  
Mi5 Networks ([www.mi5networks.com](http://www.mi5networks.com))  
Microsoft ([www.microsoft.com](http://www.microsoft.com))  
Shavlik ([www.shavlik.com](http://www.shavlik.com))  
SonicWALL ([www.sonicwall.com](http://www.sonicwall.com))  
StaySafeOnline.org  
([www.staysafeonline.org](http://www.staysafeonline.org))  
StopBadWare.org ([www.stopbadware.org](http://www.stopbadware.org))  
Sunbelt ([www.sunbelt-software.com](http://www.sunbelt-software.com))  
SurfControl ([www.surfcontrol.com](http://www.surfcontrol.com))  
Symantec ([www.symantec.com](http://www.symantec.com))  
Tenebril ([www.tenebril.com](http://www.tenebril.com))  
Trend Micro ([www.trendmicro.com](http://www.trendmicro.com))  
WatchGuard ([www.watchguard.com](http://www.watchguard.com))  
Webroot ([www.webroot.com](http://www.webroot.com))