



CMP

United Business Media

# Network Computing

9.22.2005 | WWW.NWC.COM

*For IT By IT*

# TOXIC PAYLOAD

We tested seven enterprise-class anti-spyware suites and awarded Sunbelt's CounterSpy Enterprise top honors, but Trend Micro's Anti-Spyware for SMBs will appeal to those who favor Web-based administration

BY CHRISTOPHER T. BEERS

**S**pyware isn't just annoying, it's dangerous and expensive to combat. We found some eye-popping statistics when working on this article, but one particular blog entry really illustrates the problem: Researchers at Sunbelt Software, which participated in this review, last month uncovered a large cache of detailed financial information that had been gathered by a keylogger, Srv.SSA-KeyLogger. The data was culled from apps that use HTML forms (see more at [www.sunbelt-software.com/Press.cfm?id=125](http://www.sunbelt-software.com/Press.cfm?id=125)). The FBI is investigating, and while prosecution in these cases is iffy, one thing is certain: We will see more of this sort of malware.

Now we'll tell you the secret to stopping spyware: Restrict users from installing software, period. We found that deploying users in our Active Directory with local workstation administration rights caused 100 percent of our contaminations. In our months of tests involving 30 varied pieces of spyware and other unwanted programs, not one byte was installed when we restricted user rights on the workstation. Giving users local administrator rights is a relic from



the Windows NT era, when software developers all too often didn't build applications to run within minimal-rights environments. Bottom line: Spend the money you've budgeted for anti-spyware software on deploying a minimal-rights desktop computing environment.

## Still Reading?

**For those of you who can't restrict rights** on end user workstations, we invited 25 vendors to our Syracuse University Real-World Labs® to participate in a head-to-head review of enterprise anti-spyware tools. Products had to be capable of scanning clients and eliminating malware, then protecting against new spyware-related threats in a distributed environment. What makes a product enterprise-class? Management, baby. To qualify, software suites had to be controllable from a central console, provide reporting and alerts to security administrators, and allow for scheduled and real-time scanning. Without a central management console, even the most effective anti-spyware product will be a nightmare for those supporting more than a few dozen endpoints. Getting the application on every system would be a job in itself, and at the end of the day you'd have no idea how effective your purchase was unless you monitored spyware-related helpdesk calls and extrapolated from there. No thanks.

Computer Associates, F-Secure, Lavasoft, McAfee, Sunbelt Software, Trend Micro and Webroot Software all have products that met our criteria and accepted our invitation. For a list of those companies invited but not participating, see "No Shows and No Gos," page 6.

Note that the products tested are standalone anti-spyware apps, with the exception of McAfee's VirusScan Enterprise and F-Secure's Anti-Virus Client Security, which are parts of the vendors' antivirus-plus-anti-spyware suites.

## Spyware Defined

**Spyware is a general term** used to describe unwanted, obtrusive and potentially dangerous software installed on a workstation, mostly to enrich the creator. Most vendors toss adware, BHOs (browser-helper objects), distributed attack tools, keystroke loggers, P2P software, tracking cookies and unauthorized remote administration tools into the general spyware bin. Of these, keystroke loggers, distributed attack tools and unauthorized remote administration tools are the most dangerous because they let attackers cull information as users go about their business. Keystroke loggers and remote administration tools are particularly effective at capturing business users' Web mail entries, VPN and other login credentials, corporate credit-card numbers, administration account information and other sensitive employee and/or customer information. Distributed attack tools can turn your company's computers into spam-sending relay stations or involve them in distributed DoS attacks.

Adware, P2P software, BHOs and tracking cookies

generally are more annoying than dangerous, causing pop-ups and slow browser interaction with Web sites as they track where employees travel on the Internet. Still, they reduce productivity, and P2P software, if used by employees to download music illegally, could put your organization in the crosshairs of the Digital Millennium Copyright Act.

## Spyware Evaluated

**The products' ability to detect and remove** spyware comprises 40 percent of their scores, with the remaining 60 percent split among console/client configuration, scanning in real time and on schedule, ease of managing and deploying definition file updates, reporting, alerts and notifications, and price.

The products reported on the number of items detected during scans in drastically different ways. No matter what anti-spyware software vendors say in their glossy marketing folders, the sheer number of items removed is not a valid indicator of effectiveness. In our tests, some products listed each registry-entry and file-system change as a unique item; others grouped these changes and listed them under the program(s) responsible. We saw some products detect more than 1,000 possibly unwanted programs, while others flagged fewer

## Executive Summary

# SPYWARE DETECTION

Spyware is a big problem that's only getting bigger. The only way to put a definitive halt to infections is to lock down your end users' workstations, removing all admin rights to install software. If that's impossible in your organization, then you need anti-spyware software.

We tested offerings from Computer Associates, F-Secure, Lavasoft, McAfee, Sunbelt Software, Trend Micro and Webroot Software that can be deployed from a central management console, provide reporting and alerts, and allow for scheduled and real-time scanning to prevent new infestations. McAfee's and F-Secure's products are modules of their antivirus suites and cannot be purchased separately. If you have deals with these companies, you may be able to get a good price on serviceable anti-spyware software.

However, if you want top-of-the-line protection, we found the top three standalone anti-spyware apps did a better job. We especially liked Sunbelt Software's CounterSpy Enterprise, our Editor's Choice winner, and Trend Micro's Anti-Spyware for SMBs, which came in a close second. The main difference between the two: Sunbelt has a conventional administration console while Trend's is Web-based. Either will inoculate your desktops against most spyware.

than 100, all stemming from our 30 pieces of malware. Because most spyware downloads other spyware, we examined our machines for any nonstandard processes. For comparison purposes we list the number of reported items, but for testing we evaluated the anti-spyware software by examining the computer after it was cleaned, looking for restored functionality of Internet and Windows Explorer and elimination of BHOs, unauthorized programs and pop-ups. We inspected running processes against a known-clean baseline, then used a network analyzer to watch for unauthorized traffic.

In our main scoring category, both Trend Micro's Anti-Spyware for SMBs and Sunbelt Software's CounterSpy Enterprise 1.5 performed impressively. We deployed the products on one Windows XP and one Windows 2000 workstation that were so infected they were barely usable. We weren't even able to sign into the workstations (see "How We Tested," page 5). We give a slight edge in spyware detection and removal to CounterSpy—after a single very quick scan (one of the speediest in the pool of seven products) followed by a reboot, CounterSpy restored both machines to full functionality, removing almost all unwanted registry additions. Trend Micro's Anti-Spyware also found and eradicated most of our malware. The only product we'd label deficient in this area is CA's eTrust PestPatrol. Although PestPatrol said it detected and removed 82 and 76 "pests" on the Windows 2000 and Windows XP clients, respectively, many BHOs remained on the Windows 2000 machine, several registry items were passed over, and IE still wasn't usable on the XP machine. We couldn't open the browser and experienced persistent error messages and requests to send reports to Microsoft. The functionality of both test clients was still impaired.

Besides testing the anti-spyware software's ability to detect and remove spyware, we also evaluated configuration features critical to enterprises. IT groups must be able to deploy and control the scanners from a central location and access reports on their effectiveness. This reporting also may be used to correlate access to prohibited Web sites, like gambling sites, to employee workstations that are commonly infected. These flags can then be passed from IT to the employees' supervisors.

Unfortunately, Lavasoft's Ad-Aware SE Enterprise requires login scripts or an installer on each workstation. The other products incorporate deployment capabilities into their administrative consoles, making installation a breeze. In particular, Trend Micro's Anti-Spyware stands out for its lightweight Web management console. It delivered all the functionality we would expect from an enterprise detection tool, accessible from anywhere on the network. IT managers can even access the management Web site while traveling, using a corporate VPN.

CounterSpy's more conventional management console also allows for a great deal of configuration without being too complex or bloated. In contrast, McAfee's flagship ePolicy Orchestrator (ePO) management console configuration is so highly customizable, letting us tweak every aspect of the software, that it became confusing at times.

We did find the Trend Micro product's policy-configuration options more limited than the McAfee product's, but this was true of all the pure plays, as opposed to products that are linked to antivirus suites that use mature management platforms. In fact, the specialized anti-spyware products' configuration settings, such as

REAL-WORLD  
LABS®

## REPORT CARD

## Spyware Detectors

	Sunbelt Software CounterSpy Enterprise 1.5	Trend Micro Anti-Spyware for Small and Medium Businesses 3.0	Webroot Software Spy Sweeper Enterprise 2.1	McAfee Anti-Spyware Enterprise and Active VirusScan Suite	F-Secure Anti-Virus Client Security 6.0	Lavasoft Ad-Aware SE Enterprise	CA eTrust PestPatrol Corporate Edition 5
<b>SPYWARE DETECTION AND REMOVAL (40%)</b>	<b>4</b>	<b>4</b>	<b>3.5</b>	<b>3.5</b>	<b>3.5</b>	<b>3.5</b>	<b>2.5</b>
<b>CONSOLE/CLIENT CONFIGURATION (25%)</b>	<b>4.5</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>3.5</b>	<b>3</b>	<b>3</b>
<b>MANAGEMENT/DEPLOYMENT OF DEFINITION FILE UPDATES (10%)</b>	<b>4.5</b>	<b>4.5</b>	<b>4</b>	<b>3.5</b>	<b>4</b>	<b>2.5</b>	<b>3</b>
<b>REAL-TIME AND SCHEDULED SCANS (10%)</b>	<b>4.5</b>	<b>4.5</b>	<b>4.5</b>	<b>4.5</b>	<b>4.5</b>	<b>2.5</b>	<b>4.5</b>
<b>REPORTING/ALERTS/NOTIFICATIONS (10%)</b>	<b>4.5</b>	<b>4.5</b>	<b>4.5</b>	<b>4</b>	<b>4</b>	<b>2</b>	<b>1</b>
<b>PRICE (5%)</b>	<b>4</b>	<b>4</b>	<b>3</b>	<b>3.5</b>	<b>2</b>	<b>3</b>	<b>2</b>
<b>TOTAL SCORE (100%)</b>	<b>4.28</b>	<b>4.15</b>	<b>3.85</b>	<b>3.78</b>	<b>3.63</b>	<b>3.00</b>	<b>2.70</b>
A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5 A-C GRADES INCLUDE + OR - IN THEIR RANGES. TOTAL SCORES AND WEIGHTED SCORES ARE BASED ON A SCALE OF 0-5.	<b>B+</b>	<b>B+</b>	<b>B</b>	<b>B</b>	<b>B-</b>	<b>C+</b>	<b>C</b>

Customize the results of this report card using the Interactive Report Card®, a Java applet, at [www.nwc.com](http://www.nwc.com).

definition updates, installation and scan schedules, are more limited across the board compared with the McAfee and F-Secure antivirus-plus-anti-spyware suites. However, after pitting both McAfee's and F-Secure's products against rivals that focus only on spyware removal, we found that the spyware-focused products were much more effective at eradicating malware. Frankly, this surprised us—we expected the threat analysis experts at antivirus companies to be well-versed in finding malicious software. Those who use F-Secure or McAfee for

antivirus needs should give their anti-spyware modules a test run, but others likely won't find them compelling enough to buy a bundled virus/spyware/firewall suite.

## Search and Destroy

**All the products let us perform** real-time and scheduled scans (each product uses a single scanning engine and spyware definition file for both scheduled and ad-hoc scans). We could schedule our scans nightly, weekly or monthly. Real-time scans are ad hoc, one-off

# HOW WE TESTED SPYWARE DETECTORS

Our test bed consisted of three computers: one Windows 2003 server, one Windows XP client and one Windows 2000 client, all patched with critical updates from Microsoft. All machines were members of the same Active Directory domain served from the Windows 2003 server. Users were created in the AD domain and given local admin rights on the two workstations, something all too common in corporate computing environments.

We installed the products' central management components on our Windows 2003 AD Server and deployed the anti-spyware software on each client, automatically from the AD server where possible. The central management server had to configure client settings, perform real-time and scheduled scans, manage and deploy updates of spyware-definition files, alert us to spyware outbreaks and provide reports of client activity.

To test the effectiveness of each anti-spyware program, we designed tests representative of a real-world software deployment in a business setting. Each vendor's product was run against two infected machines to see how well they removed spyware on clients.

We infected the machines with spyware that's floating around on the Internet, including items commonly found on gambling and pornographic sites—prime places for embedded spyware to be loaded. We'd catch grief from some of the makers of our test malware (and possibly our corporate legal department) if we published the names of the files. Discretion being the better part of valor (and survival), we'll leave it to your imagination.

This test was typical of an initial deployment at an enterprise with heavily infected machines and no anti-spyware application. The testing was tough on the anti-spyware products and represented an extreme example of an infected end-user desktop. We forced the software to remove spyware from computers that were so infected they were hardly usable. In fact, after infecting the computers with 30 known spyware programs and rebooting a couple of times, we couldn't even sign in! We had to manually remove a registry entry that was forcing a piece of spyware to consume all CPU resources on both clients. Internet Explorer would not even load on our Windows XP client, instead prompting a box telling us it had encountered an error and wanted to phone home to Microsoft. On the Windows 2000 client, Internet Explorer had so many search bars (called browser-helper objects, or BHOs) loaded that there were only about two inches of available screen space left for actual Web page content when browsing sites—if IE had been functioning on our Windows XP client, we suspect the same would be true there. The Windows Explorer (file-browsing) application would not start on the Windows XP client, but that's to be expected because IE and Explorer are tied together so tightly.

Besides testing the anti-spyware software's ability to detect and remove spyware, we also tested features that are critical to enterprise deployments of such software. The best anti-spyware software would be ineffective in large organizations if it

couldn't be deployed from a central location, controlled from that same location and offer some level of reporting on its effectiveness.

Measuring the effectiveness of each vendor's anti-spyware software was a challenge because spyware makes many changes to the Windows registry and file system. Spyware researchers have their work cut out for them. For our testing, indications of a clean machine included restored functionality of IE and Explorer without BHOs, inspection of running processes and services that should not be there, a Windows system tray that had no unauthorized programs and no pop-ups while using the computer. For example, after IE was started we made sure it contained no extra search bars and that it did not generate traffic to Web sites we were not browsing. Because the computers were base installs of Windows OSs, we verified that the processes in the task manager were only those that belonged on a freshly installed machine. Just to make sure we didn't miss anything, we used network analyzers to view any unauthorized traffic that remaining spyware would generate.

All NETWORK COMPUTING product reviews are conducted by current or former IT professionals in our Real-World Labs® or partner labs, according to our own test criteria. Vendor involvement is limited to assistance in configuration and troubleshooting. NETWORK COMPUTING schedules reviews based solely on our editorial judgment of reader needs, and we conduct tests and publish results without vendor influence.

scans that run immediately when initiated from the admin console. These are useful when an employee calls your helpdesk for support, but they shouldn't be confused with the active protection environment—an always-on scan—that all the products offer.

McAfee's scanner operated a bit differently when providing active protection. The company told us its active protection renders spyware useless, but it won't clean up all traces of it until a scheduled scan is done, which the company recommends you do nightly. The other products we tested provided active protection but don't take this extra precaution. Spyware software loads libraries into programs like Internet Explorer, and removing those during an active user session can cause problems, according to McAfee.

CA and F-Secure left our test machines considerably hampered after our real-time scans to remove the 30 spyware pieces. This probably was not the fault of the engines, but rather attributable to how the vendors define *spyware* in their databases. They take pains to make sure that, for example, legit remote administration tools that assist with helpdesk support aren't disabled. Sunbelt's CounterSpy, Trend Micro's Anti-Spyware and Webroot's Spy Sweeper led the pack at scanning and removing spyware threats in real time.

Also, note that *spyware* isn't *spyware* to everyone—some companies get all het up and threaten legal action if their software that is installed without the users' knowledge or permission is labeled as, gasp, *spyware* (see [netrn.net/spywareblog/archives/2005/06/12/directrevenue-responds-to-lawsuit/](http://netrn.net/spywareblog/archives/2005/06/12/directrevenue-responds-to-lawsuit/)). That's why we're not supplying a list of the 30 pieces of malware we used for testing.

## File That

We evaluated how the products managed and deployed definition files. All the products we tested downloaded their update databases to their management platforms, then deployed them to our managed clients. The

## NO SHOWS AND NO GOS

We cast a wide net for this review, inviting Allume Systems, Aluria Software, Apreo, Computer Associates, Determina, Eset Software, Finjan Software, F-Secure, Intermute, Lavasoft, McAfee, Merijn.org, Microsoft & The Giant Co., Omniquad, Panda Software, PepiMK/Spybot-S&D, Sana Security, Sunbelt Software, SurfControl, Symantec, Tenebril, Trend Micro, Webroot Software, Websense and Whole Security.

Determina said its product did not meet all our entry criteria. Eset Software and SurfControl did not participate for logistical reasons. Tenebril, Microsoft, Panda and Omniquad bowed out, citing pending new releases. The other vendors did not reply to our invitation.

# FYI

**A Cry for Help:** 20 percent to 40 percent of enterprise helpdesk calls are related to infestations of unwanted malware, according to Gartner.

downloads are automated, and a setting in the management console let us schedule them automatically. We could determine the version of definition files on all the products from the central management platform. Webroot's Spy Sweeper and McAfee's VirusScan have an edge in larger corporations because IT can deploy update client servers on the same LAN as clients, allowing for quick fixes and conserving bandwidth. We didn't run into problems rolling out new spyware definition files, but you may want to test a limited deployment.

Reporting is also critical to ensure your anti-spyware policies are doing their job. Reports generally include bar and pie charts and tables indicating the number and type of threats found on each workstation. Executive summary reports provide high-level overviews, whereas reports showing spyware discovered provide in-depth detail.

The best graphical executive summaries are from Sunbelt CounterSpy, McAfee VirusScan, Webroot Spy Sweeper and Trend Micro Anti-Spyware. In contrast, the products from CA and Lavasoft offer only text-based reporting; it's hard to extrapolate trends from these summaries. McAfee provides the most customizable reports, but to get the full benefits you must run Microsoft SQL Server. This may mean buying another software license and support contract, so if rich reporting is a must and you've chosen McAfee's product, figure that into your budget.

Most competitors offer some type of alerts and notification; this early warning can be important when a spyware outbreak occurs. Only two products, those from McAfee and F-Secure, provide alerts over SNMP that integrate with central alerting and monitoring tools. All others rely on e-mail or pop-ups on administrator desktops, which we found acceptable. Sunbelt allows end-user pop-up notification, but we think that may confuse users and increase helpdesk calls. We could forward most alerts to SMS-capable cell phones or text pagers.

## Final Tally

**Sunbelt CounterSpy Enterprise** wins our Editor's Choice award for its modern interface design, ease of deployment and ability to remove what we threw at it. Trend Micro's low-priced Anti-Spyware for SMBs and Webroot's Spy Sweeper Enterprise were hot on Sunbelt's heels, though, and are good choices for any enterprise. Those partial to Web administration consoles should look at Trend Micro's offering.

McAfee's Anti-Spyware Enterprise and F-Secure's Anti-Virus Client Security are modules of these companies' Active VirusScan and Policy Manager suites, respec-

tively. Shops that have relationships with these vendors will find both functional but not up to the level of our three leaders. Anti-Spyware Enterprise was the only product we tested to offer role-based administration, but it cannot undelete mistakenly removed items.

Lavasoft's Ad-Aware SE Enterprise and CA's eTrust PestPatrol Corporate Edition brought up the rear. Ad-Aware lacks a quarantine function that would let admins undo mistaken removal of necessary elements, and we found it hard to deploy. CA's PestPatrol was hurt by its inability to restore our test machines to working order, high purchase price and text-only reporting.

We set a pricing scenario of 1,000 users and requested

24/7 support for one year. Prices ranged from a low of \$11 per user to a high of \$17.28, with an average of \$14.28 per user. One year's support was included; thereafter, support averaged 30 percent of the purchase price. Remember that this software is subscription-based—recurring charges generally average 30 percent of the initial purchase price each year after the first. When budgeting, nail down ongoing costs.

**Sunbelt Software CounterSpy Enterprise 1.5** It wasn't easy to declare a winner, but CounterSpy Enterprise covered all the bases from our systems administrator's point of view. Its spyware detection and prevention were excellent.



## SPYWARE DETECTOR VENDORS AT A GLANCE

### PUBLIC COMPANIES

Company name (stock symbol)	Year founded	Product name	Year launched	Market capitalization as of Sept. 1 \$000	Other products	Key customers
<b>COMPUTER ASSOCIATES INTERNATIONAL (CA)</b>	1974	eTrust PestPatrol Corporate Edition r5	2004	\$15,690,000	BrightStor CA, Unicenter CA, AllFusion, Advantage	AAA Reading-Berks, Brigham Young University, Challenger TAFE, Chapman Tripp, Fujitsu Services, MilanLab, Rex Healthcare, SECOM Trust.Net
<b>F-SECURE (FSC1V)</b>	1988	Anti-Virus Client Security 6.0, Policy Manager 6.0	1999	N/A	Anti-Virus Small Business Suite, Anti-Virus Enterprise Suite, Anti-Virus Corporate Suite, Anti-Virus Mail Server and Gateway Products, Anti-Virus for Workstations, Anti-Virus for File Servers, Anti-Virus for Citrix Servers	Barclays Bank, Cap Gemini, Cisco, Deutsche Telekom, Ernst & Young, Honda, IBM, Siemens AG, Sonera, Tesco
<b>MCAFFEE (MFE)</b>	1992	Anti-Spyware Enterprise, Active VirusScan Suite	2005, 2000	5,008,000	Secure Internet Gateway, IntruShield 4010 IPS Appliance	Campbell Soup, Comcast, Constellation Energy Group, Mercy Corps, Shelbyville Schools
<b>TREND MICRO (TMIC)</b>	1988	Anti-Spyware for Small and Medium Businesses 3.0	2005	4,076,000	OfficeScan 7.0, InterScan Web Security 2.5 with Damage Cleanup Service	ADC Telecommunications, EMI Music, Epson, Honeywell, Siemens AG, The Bear Stearns Co.

### PRIVATE COMPANIES

Company name	Year founded	Product name	Year launched	Employees	Other products	Key customers
<b>LAVASOFT</b>	Established in Germany in mid-1990s, incorporated July 2002	Ad-Aware SE Enterprise	2005	Undisclosed	Ad-Aware Plus, Ad-Watch, Process-Watch, RegHance	Undisclosed
<b>SUNBELT SOFTWARE</b>	1994	CounterSpy Enterprise 1.5	2004	120	iHateSpam for Exchange Sunbelt Network Security Inspector, LanHound, ServerVision, Directory Inspector. Other home office/small office products: CounterSpy, iHateSpam	Charter Bank, Congoleum, Cornell University, Digital Infrastructure, Dow Jones & Co., Grubb & Ellis, Microsoft, Northrop Grumman, University of Wisconsin, Vanderbilt University
<b>WEBROOT SOFTWARE</b>	1997	Spy Sweeper Enterprise 2.1	1994	275	PavLight 2xE1, PavLight 4xE1 integrated FSO links	Accor (parent company of Motel 6 and Red Roof Inn), University of Florida, Memorial Hospital

CounterSpy told us it detected 105 “threats” on the Windows XP client and 132 on the Windows 2000 machine and restored both test PCs to good health quickly. After a single scan we found that our browsers, which had been weighed down by multiple unwanted toolbars and other BHOs, were devoid of nonstandard “search assistants.” The number of unwanted running processes also was drastically reduced, more so than with the other products we tested.

Another critical area where CounterSpy more than exceeded our expectations is in centralized management. The Counterspy Enterprise Admin Console let us easily create policies, deploy agents, configure automated scanning and updating, and generally observe

**FYI**

**Getting Worse, and Fast:** Enterprise PCs have an average of 27 pieces of spyware on their hard drives, a 19 percent increase in the past quarter alone, while a whopping 80 percent of corporate computers host at least one instance of unwanted software, whether that’s adware, spyware or a Trojan horse, according to WatchGuard.

the status of the machines on which the product had been deployed. When creating the policy that we deployed to our workstations, for example, Enterprise Admin let us control which locations and files were scanned, specify threats to be excluded from removal, set up notifications, and configure what we wanted to do with the spyware it found. Enterprise Admin Console’s speedy installation and deployment, clean and lightweight feel, and focus on quick, intuitive access to scanning, updates, network monitoring and reports won us over. Viewing reports required no more than a couple of clicks, and Enterprise Admin gave us detailed information on the threats contained in its database.

Installation was easy, and CounterSpy accurately detected our test bed Active Directory structure and both client machines. We didn’t change the default policy because we found the out-of-the-box settings suitable for our tests, but we could have turned off spyware checking of cookies, registry entries and processes. Although we wouldn’t recommend that approach, it’s nice to have the flexibility.

We downloaded and updated agent components and threat database files easily on our test systems. Agent deployment was especially rapid, and we liked having a status bar that provided clear data on when agents were finished installing. We could choose to schedule fully automated scans, or we could target specific computers or the entire enterprise for on-demand scanning. On-demand scanning, like deploying agents, includes a status bar that provides feedback on the status of the scan. This may not seem like a big deal, but it was sorely missed on some of the other products, like McAfee’s.

CounterSpy includes a powerful Active Protection feature, which monitored changes to our systems to determine possible threats. We could configure this process as well through the admin console. Part of what makes this product so effective is Sunbelt’s CounterSpy Research Center, a team dedicated to tracking down the latest threats and updating the Sunbelt threat database. We also were impressed by Sunbelt’s ThreatNet spyware reporting system (available to CounterSpy customers and included with every seat). It offered the best reporting in this review. Using Crystal Reports we could generate any of seven predefined reports that included post-scan information on infected machines, machine history, a list of threats found and an execu-



**News**

Cut 800 employees last month, but financials seem on the upswing following 8 percent revenue jump in fiscal Q1 2006

Q1 2005 fiscal revenue up 39 percent over 2004, due to increased sales in consumer market

Reported \$245 million in revenue for fiscal Q2 2005, up 32 percent from 2004

Operating income down 13 percent in fiscal Q2, due to increased support costs at company headquarters in Japan

Source: Company reports, Yahoo.com

**News**

Signed partnership in April with PIVX, provider of active systems hardening for Windows PCs

In July, hired renowned antispymware expert Patrick Jordan, aka “webhelper”

Experienced strong growth in educational market, deploying 650,000 licenses at 300 educational institutions between June 2004 and June 2005

Source: Company reports

tive summary. We could present our data as numeric values, bar graphs or pie charts.

Given its all-around excellent performance, we expected CounterSpy to be expensive. Instead, at just \$11 per user in our scenario, CounterSpy is one of the most aggressively priced anti-spyware products on the market.

CounterSpy Enterprise 1.5. Sunbelt Software, (800) 688-8404, (727) 562-0101. [www.sunbelt-software.com](http://www.sunbelt-software.com)

**Trend Micro Anti-Spyware for Small and Medium Businesses 3.0** Although Sunbelt took the top prize for this review, Trend Micro's Anti-Spyware (formerly

**B+** an Intermute product) came in a very strong second. In fact, it was only our preference for CounterSpy's client-server management console that tipped the scale. The CounterSpy interface is a conventional Windows object, whereas Trend Micro's is Web-based. We think systems administrators would prefer an interface that more closely emulates the usual Microsoft management environment. In the end, though, that's a matter of personal choice—some will prefer Trend Micro's excellent Web management console that can be accessed from any physical location on the network, or remotely over a VPN.

Trend Micro says Anti-Spyware delivers best-in-class spyware detection and removal. We couldn't agree more, and it does it at a price that's as low as CounterSpy. Anti-Spyware excelled in all six major testing areas, especially in the critical detection and removal category. This tool synced quickly with our Active Directory to detect our test client machines, and deployment and installation status bars showed us exactly what was happening and let us know when agents were completely deployed. During our tests we had some initial difficulty deploying to our Win2K client, but resending the package solved the problem. We could launch scans from the Web console on a scheduled or on-demand basis. The on-demand capabilities of this product were particularly appealing—we felt that we were in the driver's seat, capable of controlling scans to any number of machines. As it scanned our systems, Anti-Spyware reported back to the Web console what it was doing at all times.

Anti-Spyware removed our standard 30 pieces of malware to the extent that both test machines were restored to full functionality. On the Windows 2000 machine, it listed 71 threats as found and 1,135 items as cleaned. On the Windows XP machine, it found 74 threats and cleaned 1,116 items. In both cases, all spyware-related toolbars were removed from our browsers, and all other programs loaded normally. The Trend Micro product not only removed almost all known spyware files from the client machines, but it also removed most of the malicious programs that were acting as hosts to install them.

Another attractive feature is that the product runs invisibly in the background on client machines, which

## BY THE NUMBERS

In January 2005, Forrester surveyed 200 technology decision-makers about their approach to IT security.

**4th**

Where respondents ranked spyware on a list of 9 possible threats to the organization

**80**

Percentage of companies that use anti-spyware tools

**65**

Percentage of companies that will purchase or upgrade their anti-spyware software this year, making anti-spyware tools the most purchased security technology in 2005

**39**

Percentage of respondents who couldn't estimate how many systems in their organization were infected with spyware

Source: Forrester Research

means fewer helpdesk calls from users confused by warning messages. You don't want to burden your end users with spyware-detection concerns, and chances are, most users in a Trend Micro-protected environment won't even be aware of its presence.

The Anti-Spyware policy-based management console let us perform updates, application monitoring and automated scanning, and the product's reporting capabilities were excellent. We could choose from online or printed reports that are generated through MySQL. As with the other best-in-class products in this review, the reports provide colorful charts and can be configured in multiple ways.

**Trend Micro Anti-Spyware for Small and Medium Businesses 3.0.** Trend Micro, (800) 228-5651, (408) 257-1500. [www.trendmicro.com](http://www.trendmicro.com)

**Webroot Software Spy Sweeper Enterprise 2.1** Another heavy hitter in this review is Spy Sweeper. It

**B** was easy to deploy; we could choose a login script, an internal software management system or a group policy in Active Directory. As with all the products we tested, we used Active Directory. Integration with our test network was seamless, and Spy Sweeper detected our client PCs immediately. The management console was lightweight and easy to manage. Client deployment to both machines was quick, and we were greeted with status indicators and a decisive green check when deployment finished.

Webroot maintains a comprehensive database of current threats, and Spy Sweeper made it easy to get the latest updates and definitions, both manually and automatically using the administration console and a click of the mouse. We could scan clients manually at will,

or we could schedule scans to run as a fully automated process. Like the other favorites in this review, Spy Sweeper offered status indicators during sweeps to let us know exactly what was happening.

Spy Sweeper did a solid job removing our 30 pieces of spyware and preventing re-infection. After our test

sweep, both machines were again operational. Browser functionality was restored in both cases, with only one remaining toolbar on the XP machine. In its initial sweep of our clients, Spy Sweeper said it detected 166 and 177 items, respectively, on the Windows 2000 and XP machines. Because of Webroot's commitment to

## Spyware Detector Features

	CA eTrust PestPatrol Corporate Edition 5	F-Secure Anti-Virus Client Security 6.0	Lavasoft Ad-Aware SE Enterprise	McAfee Anti-Spyware Enterprise and Active VirusScan Suite	Sunbelt Software CounterSpy Enterprise 1.5	Trend Micro Anti-Spyware for Small and Medium Businesses 3.0	Webroot Software Spy Sweeper Enterprise 2.1
<b>Types detected</b>							
Spyware/adware	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y
Cookies/worms	Y/Y	Y/Y	Y/Y	Y/Y	Y/N	Y/Y	Y/N
Trojan horses	Y	Y	Y	Y	Y, Trojan downloaders	Y	Y
Keystroke loggers	Y	Y	Y	Y	Y	Y	Y
Hacker tools	Y	N	Y	Y	Y	Y	Y
P2P applications	Y	N	N	Y	Y	Y	N
Games	Y, if contains malware	N	N	Y	Y, if bundles adware or spyware	N	N
Remote administration tools	Y	Y	N	Y	Y	N	Y
<b>Spyware detection methods</b>	Signatures, patterns, md5, heuristics, CRC	Signature, patterns, heuristics	Signatures, fingerprints, CRC/md5-like	Signatures, patterns, md5, heuristics	Signatures, md5	Signatures, patterns, md5, heuristics, process start-up	Signatures, patterns, md5, heuristics, Phileas technology
<b>Spyware removal methods</b>	Quarantine, clean, delete, prevent	Quarantine, clean, delete, prevent, allow	Quarantine, clean, delete, prevent	Quarantine, clean, delete, prevent, deny access	Quarantine, delete, prevent	Quarantine, clean, delete, prevent	Quarantine, clean, delete, prevent
<b>Active spyware protection</b>	Y	Y	Y	Y	Y	Y	Y
<b>Performs scheduled/real-time scans</b>	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y
<b>Undeletes mistakenly removed spyware/by whom</b>	Y, if quarantined/ by admin	Y, with quarantine/ by user	N	N	Y, using quarantine/ by admin	Y/by admin	Y/by admin
<b>Administration</b>							
Web-based console	Y	N	N	N	N	Y	Y
Client/server-based console	Y	Y	Y	Y	Y	Y	Y
Role-based administration	N	N	N	Y	N	N	N
<b>Reports and alerts</b>							
Web-based reports	N	Y	N	N	N	Y	Y
Client/server-based reports	Y	Y	Y	Y	Y	Y	Y
Customized text-based reports	Y	N	N	Y	N	N	Y
Customized graphical reports	N	N	Y	Y	N	N	Y
Customized e-mail alerts	Y	Y	Y	Y	Y	N	Y
Customized SNMP alers	N	Y	N	Y	N	N	N
Other types of alerts	N	N	N	Y	Y	N	N
<b>Standalone software (no additional purchase required)</b>	Y	N	Y	N	Y	Y	Y
<b>Price per user for 1,000-user license</b>	\$17	\$17.28	\$15.95	\$12.40	\$11	\$11	\$15.28
<b>24/7 support for 1,000-user license</b>	Included in per-user price	N/A	1st year included, 35% of purchase price thereafter	\$4.96 per user, 2nd and 3rd years	1st year included, 25% of purchase price thereafter	\$3,995	1st year included, 30% of purchase price thereafter

Y=Yes, N=No

keeping track of the latest threats and updating its database, the results of the test scan were impressive.

A particularly strong attribute of Spy Sweeper is its detailed reports, which let us dig into and analyze our results. Like Trend Micro's Anti-Spyware, Spy Sweeper can use a SQL Server database, but it also comes with a prepackaged database of its own for those not running SQL. A nice touch.

Spy Sweeper's management console offers a range of configuration options, but with a focus on simplicity. Updating definition files was fast, and it was easy to cascade the updates to the enterprise environment simply by dragging and dropping. The admin console user interface made it easy to configure and push client installs, simply by checking empty boxes next to highly visible client icons. Add scan scheduling and clear alert notifications, and we found this to be an appealing and easy-to-use management interface.

Spy Sweeper Enterprise 2.1. Webroot Software,  
(800) 772-9383, (303) 442-3813.  
[www.webroot.com](http://www.webroot.com)

### McAfee Active VirusScan Suite and Anti-Spyware Enterprise Software

The centerpiece of McAfee VirusScan is its ePolicy Orchestrator management console.

**B** In testing we found VirusScan Enterprise to be a powerful tool with which systems administrators can manage virus and spyware protection across the enterprise. However, to use its anti-spyware service, you must have the antivirus component installed—McAfee VirusScan is a complete security suite, with spyware protection making up just a portion of the package. This is a benefit if your enterprise runs McAfee as its antivirus application. If not, it will be difficult to justify switching to McAfee just for spyware protection.

Although we like the ePolicy Orchestrator console, Anti-Spyware Enterprise took substantially longer to install than rivals. This was most likely caused by the default polling period that ePO used to check in with its agents installed on the workstation. As with the other products we tested, we set up the ePO to recognize our client machines by identifying Active Directory containers, and it located our Windows XP and 2000 machines with ease.

As its name suggests, ePO let us configure a security policy that is inherited across the network. Of all the products we tested, McAfee allowed for the greatest degree of customization in terms of policy management. For this test, we configured a policy for our client machines before deployment. We were disappointed, given the slowness of the install, that there's no way to determine the progress of an installation or deployment until the agent is polled again.

Anyone familiar with antivirus products knows definition files must be downloaded periodically to keep antivirus and anti-spyware definitions up to date, and with Anti-Spyware Enterprise it was easy to config-

**FYI**

**No. 1 Threat:** Two-thirds of IT professionals and security administrators surveyed by WatchGuard say spyware is the top network security threat this year. Viruses, with 23 percent, and phishing, with 10 percent, follow.

ure our client machines with automatic updates.

The results of the McAfee scan indicated that 733 total items were detected on the Windows 2000 machine, while 1,145 items were found on the XP machine. Although this scan eliminated most of the malware installed, a small spyware footprint remained. However, the McAfee product did restore full functionality to both client machines. Browsers were restored to their original states, browser helper toolbars were removed, and we saw a drastic reduction in unwanted registry items.

McAfee Anti-Spyware Enterprise and Active VirusScan Suite. McAfee, (888) 847-8766.  
[www.mcafee.com](http://www.mcafee.com)

### F-Secure Anti-Virus Client Security and Policy Manager 6.0

As with McAfee's product, the concept of integrating anti-spyware into a flagship antivirus pack-

**B** age has both pluses and minuses. On the plus side, if yours is an F-Secure house, installing the anti-spyware add-on is a logical choice. If, however, you use some other enterprise antivirus application, you'd need a compelling reason to make the switch. Just like McAfee's suite, the F-Secure anti-spyware package is dependent on the parent antivirus program, and buying the item alone is not an option.

Anti-Virus Client Security (AVCS) made a so-so showing in the critical area of spyware detection and removal, faring slightly worse than McAfee's product and leaving much to be desired compared with the top performers in this review. After our initial scan and reboot, client machine performance was still significantly hampered. AVCS identified and removed 133 and 198 instances of malware on our respective Windows 2000 and XP client test machines. F-Secure's scanning engines removed several unwanted programs, but browser functionality was still disabled on one client, while a BHO remained in the other.

The dominant feature of the F-Secure product is its management console. In addition, F-Secure Client Security integrated seamlessly with Active Directory and allowed for easy deployment of packages to our detected clients. An added bonus is AVCS's integrated firewall, though we wish it didn't pop up quite so prominently on the end-user desktop; we foresee some confusion. F-Secure's product easily met our testing criteria with its four scanning methods: real-time scanning, e-mail scanning, Web traffic scanning and manual scanning.

One of our gripes with the F-Secure offering is that it took a long time to push packages and updates to our client machines. However, AVCS is a top performer in terms of ease of use and effectiveness as a systems man-

## FYI

**Throw It In:** At a Gartner summit in June, 41 percent of attendees with more than 500 desktops said they get their anti-spyware software at no cost from their desktop antivirus vendors. Gartner projects that this number will grow to 60 percent by year's end and to 95 percent by the end of 2007.

agement tool. The Policy Manager let us create highly customized, detailed policies concerning installation, types and times of viruses and spyware scanned, actions taken, reporting and notification. To round out the review of this Finnish antivirus product, we would stress that the anti-spyware component is a satisfactory compliment to the F-Secure total package.

Anti-Virus Client Security and Policy Manager 6.0.  
F-Secure, (408) 938-6700. [www.f-secure.com](http://www.f-secure.com)

**Lavasoft Ad-Aware SE Enterprise** We move from Finland over to Sweden and well-known anti-spyware



vendor Lavasoft. This brand is readily recognizable to many because of its strong reputation as a leading provider of free anti-spyware to the consumer market. The product tested in this review, Lavasoft Ad-Aware SE Enterprise, is a combination of Lavasoft's Ad-Aware SE Professional Edition and the Ad-Axis Management Console.

Ad-Aware SE did an excellent job eradicating spyware from our test machines. There is no doubt the scanning technology works. Unfortunately, throughout all phases of testing, Ad-Aware SE seemed as if it were a cobbled version of its two parts, rather than an integrated whole. In fact, this was the only product we tested that required us to install the client software on each machine by hand. We actually needed to configure three separate items for the product to work: the Ad-Axis Management Console, the Ad-Axis clients and the Ad-Aware software. Of course, the Ad-Aware component could easily be deployed to client machines using start-up scripts, but this solution is still much more involved than what rivals had to offer. This factor, more than anything, pulled Ad-Aware out of contention for one of the top spots in this review.

In terms of overall functionality, Ad-Aware SE does meet all of the testing criteria. Once we had it set up and configured properly, the product performed admirably in the detection and removal of unwanted objects. Our initial scan and reboot showed that Ad-Aware SE detected 166 and 177 objects on the respective Windows 2000 and XP machines. Almost all unwanted programs and registry items were removed, and the functionality of browsers in both client machines was restored. Its Ad-Watch feature provided real-time monitoring of our end-user environment, and Process-Watch allowed for viewing and termination of running processes. In the current version, notifications are available through e-mail only, but this will likely change in future iterations.

Another area where Ad-Aware SE will need significant improvement to compete with the big dogs is its

reporting capabilities. The polished reports offered by its competitors just weren't there. In fact, text files were the main source of information available following a scan, and this format is difficult to use when information is needed quickly.

Although we consider Ad-Aware SE not quite ready for enterprise-level service, it's an excellent spyware removal tool, and we'll be watching to see whether future releases move toward a more integrated package.

Ad-Aware SE Enterprise (combination of AD-Aware SE Professional and Ad-Axis Management Console).  
Lavasoft, +358-9-693-2220. [www.lavasoft.com](http://www.lavasoft.com)

**Computer Associates International eTrust PestPatrol Corporate Edition 5** CA's eTrust PestPatrol is an easy-to-use tool that deployed well and met all testing



criteria, but it was deficient in detecting and removing spyware. The PestPatrol management console found our client machines without a hitch. CA's anti-spyware engine is based on Microsoft's .Net infrastructure and is advertised as able to access a wide range of known malware. However, our testing showed that it wasn't as effective as rivals: The CA product detected and removed 82 and 76 "pests" on the respective Windows 2000 and Windows XP clients. But numerous BHOs remained on the Windows 2000 machine, several registry items were passed over, and IE wasn't usable on the XP machine. The browser would not open, there were persistent error messages, and we were deluged with requests to send error reports to Microsoft.

As with Lavasoft's reports, those produced by CA's product could not compare with the leaders in this review. PestPatrol's reports, while thorough, are provided in a simple text format that won't impress the front office.

Still, PestPatrol did excel in a number of areas. In terms of syncing with Active Directory, it really couldn't have done better. The installation and configuration aspects of our testing were impressive in that each step was accentuated by status bars. The process of "pushing" spyware detection software to our two client machines was easier than on any other tested product. We simply checked a box and the client packages were deployed. From an end user perspective, PestPatrol is invisible on the client, which means fewer calls to the helpdesk.

PestPatrol let us create start-up, scheduled and on-demand scans from the management console and, in general, provided intuitive feel, ease of deployment and quick configuration. But it was weak in the most important area: spyware detection and removal.

eTrust PestPatrol Corporate Edition 5. Computer Associates International, (800) 225-5224, (631) 342-6000. [www.ca.com](http://www.ca.com)

