

INFORMATION SECURITY®

PRODUCT REVIEW

spy catchers

We take a close look at seven enterprise antispymware products. Can they keep your corporate desktops free of prying eyes?

BY ED SKOUDIS & TOM LISTON

SPYWARE HAS MANY ORGANIZATIONS CRYING “UNCLE!” HELP DESKS are inundated with user complaints about incessant ads, slow system performance and dysfunctional machines. In response, many companies are deploying enterprise-wide antispymware products, finding that the easily quantifiable savings justify the expenditure.

Yet, help desk costs are the least sinister aspect of the spyware menace. Worst-case scenarios include the disclosure of sensitive corporate secrets or the theft of employees’ personal information. Whatever the business case for deploying antispymware, the market has grown quickly. Antispymware companies have scrambled to extend their consumer offerings into centrally managed enterprise products, and antivirus providers have developed—or acquired—antispymware capabilities.

a closer look at this review

						
CA's eTrust PestPatrol Anti-Spyware 8.0	eSoft's Desktop Anti-Spyware 1.2	Lavasoft's Ad-Aware SE Enterprise Edition 1.7	McAfee's AntiSpyware Enterprise 8.5	SurfControl's Enterprise Threat Shield 3.0	Trend Micro's Anti-Spyware Enterprise Edition 3.0	Webroot Software's Spy Sweeper Enterprise 2.5

Information Security tested seven enterprise desktop antispymware products from CA, eSoft (licensed from Aluria Software), Lavasoft, McAfee, SurfControl, Trend Micro and Webroot to determine their management capabilities, behavior- and signature-based detection and resilience to attacks. (Shavlik Technologies, Sunbelt Software, Symantec and Tenebril declined to participate, all citing anticipated improvements in upcoming releases available after our test period.)

Our test bed consisted of a Windows 2000 management

server controlling three Windows XP Pro workstation systems. We tested each product using 54 common spyware specimens, including keystroke loggers, pop-up ad generators and browser hijackers. Further, we created a custom suite of spyware applications, dubbed SPYCAR (available for download at www.intelguardians.com/spycar), to test behavior-based detection when no signature is available. For each product, we tested real-time protection during both copying and running spyware, as well as on-demand scanning of the complete system. ▶

Enterprise-level antispymware is a young technology—the first centrally managed products appeared about two years ago. To see if it's ready for prime time, *Information Security* tested seven desktop antispymware tools designed for business environments: CA's eTrust PestPatrol Anti-Spyware 8.0; eSoft's Desktop Anti-Spyware 1.2. (an OEM rebranding of Aluria Software's Paladin); Lavasoft's Ad-Aware SE Enterprise Edition 1.7; McAfee's AntiSpyware Enterprise 8.5; SurfControl's Enterprise Threat Shield 3.0; Trend Micro's Anti-Spyware Enterprise Edition 3.0; and Webroot Software's Spy Sweeper Enterprise 2.5.

In our lab, we analyzed and graded their capabilities (*see "Making the Grade"*) for enterprise management, resistance to common attacks, evasion techniques, and the ability to detect spyware using both behavior- and signature-based mechanisms.

Enterprise Management

The ability to control antispymware tools across an enterprise is crucial. If a product can't be managed remotely and in large numbers, it just isn't useful to enterprises. We compared several aspects of enterprise management:

Policy definition and grouping. Each of the antispymware products allows administrators to define policies by setting scan schedules, specifying quarantine and delete options, and tweaking scan configurations. While such options are useful, the ability to apply policy to grouped systems is critical in large, growing deployments.

McAfee offers the most comprehensive policy configuration options, allowing fine-grained control over scan schedules, real-time alerting and user interface configuration, with different policies allowed for arbitrary groups of machines. These features are then coupled with an excellent framework for application through McAfee's bundled ePolicy Orchestrator. This powerful and intuitive interface allows admins to define policies for specific networks, domains, ad hoc groups and subgroups. Moving systems from one policy to another requires a simple drag and drop, and the object-oriented inheritance of policies by subgroups facilitates managing large deployments.

CA offers flexible policy definitions and grouping options. However, fewer scan options can be tailored with CA's eTrust Integrated Threat Management Console, which isn't nearly as intuitive as McAfee's and seemed significantly more sluggish. It was harder to determine if and when policies were actually applied to a given host.

While eSoft, SurfControl and Webroot support applying policies by group, no subgroup options are available, limiting their flexibility and appeal to large organizations. Trend Micro offers only a flat listing of machines, limiting its scalability beyond several hundred managed systems. Larger installations require Trend Micro's Control Manager.

Lavasoft's enterprise management abilities are extremely limited. The enterprise GUI allows admins only to define update intervals and schedule on-demand scans of either all enterprise systems at the same time or a single machine. The enterprise server can't group client machines, nor can it control any of the real-time detection mechanisms of the clients, which are off by default. Lavasoft's enterprise solution appears to be a simple GUI that has been stripped down to minimal protections by default and slapped on to its consumer product.

Controlling interaction with users. Given the business case for reducing help desk calls, all the products follow this cardinal rule: "Thou shalt not interact with the user." Messages indicating spyware trouble that are displayed to the user might cause yet another help desk call, so such interaction was turned off by default.

Some of the vendors offer options for increased interaction, such as allowing the user to order an on-demand scan or to see alert messages, while others offer no user interface at all. We believe that there can be value in giving enterprises the option to allow users to conduct a full scan, perhaps saving a help desk call.

McAfee offers the most flexibility in configuring user interaction, giving admins fine-grained control to display or turn off components of the user GUI, including the ability to launch scans. McAfee also lets admins define a password for administrative control to the client, so a roving troubleshooter can correct a problem.

safer@home

Most of the vendors whose enterprise products we tested also market a consumer-grade antispyware product. In fact, most enterprise antispyware tools are repackaged consumer products, with a management front end. At the outset of our testing, we expected that the enterprise tools would offer at least the same level of protection as the consumer products, but we were wrong. In every case where a vendor supported behavior-based detection, the enterprise tool was far weaker by default than the consumer product.

Vendors told us they feared breaking corporate applications, and thus purposely dumbed down their protection for enterprise customers.

Bottom line: If you've fallen in love with a consumer antispyware product at home, don't assume that you will have the same protection from the same vendor in your enterprise. •

—ED SKOUDIS & TOM LISTON

Webroot offers the choice of a pop-up or minimized icon in the tool tray for allowing or prohibiting user-initiated scans. Similarly, eSoft displays a tool tray icon to let a user start an on-demand scan—if an enterprise wants to enable this option.

CA's only interaction with users is to pop up a request message when the enterprise management console initiates a scan, giving users an option of delaying the scan by several minutes so that they can save their work. Trend Micro and SurfControl won't allow user scans or display anything when a scan starts up; Trend Micro's obscure command-line scan initiation is helpful for support personnel.

Lavasoft offers no user interaction configuration by default, opting to keep the user out of the process. But, an adventurous user can easily find Lavasoft's directory under Program Files and invoke various .exe files to run or alter Lavasoft's installation. This is another indication that the management GUI is an overlay of the consumer product.

Reporting. Enterprise managers need access to a wide range of information about the status of their antispyware operations, from overviews of infection status all the way down to detailed reports of particular infection and containment actions.

McAfee offers the most comprehensive set of built-in reports, with enterprise-wide summaries and detailed system-by-system breakdowns. SurfControl's built-in reports are solid, but not as comprehensive as McAfee's. In particular, SurfControl splits on-demand and real-time detection into separate reports.

CA's reports offer the information we expected, with nice management summaries, such as top 10 lists of infected machines, spyware specimens and infected users. Trend Micro offers a good set of reports, which seem to be more management-focused than offering fine-grained details on individual machines. We liked its report breakdowns by category of spyware, including keystroke loggers and browser hijackers. Webroot's reports don't include any behavior-based detection results; the data is stored in log files at the client. But, the product's on-demand scan reports are solid, offering a list of the most infected machines and most prominent spyware specimens.

eSoft's reports are essentially text-based outputs of scans. Lavasoft's reports are the most disappointing—just summaries of enterprise-wide scans, without any detail about the particular spyware that was detected and what action was taken (e.g., quarantine, delete).

Finally, because several of these products use a back-end SQL database for logging report data, they support highly customized report gen-

eration using third-party tools. eSoft, McAfee and SurfControl work with MSDE, which is included, for smaller deployments, or Microsoft SQL Server. Webroot's default install uses DBISAM for smaller installations, and supports SQL Server. Trend Micro relies on MySQL and supports its interfacing query tools.

CA's proprietary back-end database offers no support for third-party SQL query tools, which reduced its grade. Lavasoft doesn't store any detailed information on the server, so it isn't useful for third-party query tools.

Behavior-based Detection

Behavior-based detection is a double-edged sword: While it improves detection, it increases the likelihood of false positives, which could break an unusual but legitimate enterprise application. Still, there's great value in blocking or alerting on suspect behavior.

Based on our experience with AV tools, we fully expected the antispyware products to have heuristic or behavior-based detection abilities to cope with a rapidly morphing threat. However, McAfee is the only one that

detected any of our tests in its default configuration; eSoft, Lavasoft and Webroot turn off behavior-based detection by default; and CA, SurfControl and Trend Micro have no behavior-based detection capabilities. Because many enterprises run security software with a default configuration, you'll have to consider your own policy.

To test behavior-based detection, we created 25 small custom programs, each of which attempted to perform a single spyware-like behavior. We dubbed the collection "SPYCAR" in homage to the well-known EICAR antivirus test file.

Our SPYCAR specimens tested each antispyware tool's ability to detect the following:

- The addition of new registry values or start menu entries to run programs loaded by SPYCAR.
- Various changes to the "Internet Options" panel in IE (including changes that lock out users' ability to change their home page).
- Changes to the home page of both IE and Firefox.
- Additions to the hosts file.
- The launch of a keylogging application.
- Addition of a browser helper object (BHO) to IE.
- Changes to the default wallpaper.

We were quite surprised to discover how few of these spyware-like behaviors were detected or blocked (*see "Behavior-Based Spyware Detection"*).

Interestingly, McAfee's default settings block programs from being run from IE's "Temporary Internet Files," a simple protection that can defeat many "drive-by" spyware installs.

eSoft, Lavasoft and Webroot produced a mixed bag of results when behavior-based detection was enabled. Webroot detected and blocked attempts to install values under the "Run" and "RunOnce" keys in HKCU and HKLM, which are often used to start spyware automatically at system boot or user logon. However, Webroot completely missed additions to RunOnceEx, a registry key that operates in much the same fashion as RunOnce. By blocking only two of the three most commonly used registry keys for launching spyware, Webroot missed a major portion of the defensive puzzle.

Lavasoft's behavior-based detection has to be enabled on each individual client. When set to its highest level of detection, Lavasoft alerted the user to an attempt to install a value under RunOnceEx and even

behavior-based spyware detection

	CA	eSoft (Aluria)	Lavasoft	McAfee	SurfControl	Trend Micro	Webroot
IE: Lock home page	●	●	●	●	●	●	●
IE: Remove "Advanced" Tab	●	●	●	●	●	●	●
IE: Remove "Connections" Tab	●	●	●	●	●	●	●
IE: Remove "Content" Tab	●	●	●	●	●	●	●
IE: Remove "General" Tab	●	●	●	●	●	●	●
IE: Remove "Privacy" Tab	●	●	●	●	●	●	●
IE: Remove "Program" Tab	●	●	●	●	●	●	●
IE: Remove "Security" Tab	●	●	●	●	●	●	●
Drop file; HKCU Run	●	●	●	●	●	●	●
Drop file; HKCU RunOnce	●	●	●	●	●	●	●
Drop file; HKCU RunOnceEx	●	●	●	●	●	●	●
Drop file; HKLM Run	●	●	●	●	●	●	●
Drop file; HKLM RunOnce	●	●	●	●	●	●	●
Drop file; HKLM RunOnceEx	●	●	●	●	●	●	●
Start Menu - All Users	●	●	●	●	●	●	●
Start Menu - Current User	●	●	●	●	●	●	●
Explorer wrapper	●	●	●	●	●	●	●
Change wallpaper	●	●	●	●	●	●	●
KeyLogger	●	●	●	●	●	●	●
Change IE home page	●	●	●	●	●	●	●
Change FF home page	●	●	●	●	●	●	●
Add an IE favorite	●	●	●	●	●	●	●
Add an entry to the hosts file	●	●	●	●	●	●	●
BHO	●	●	●	●	●	●	●

LEGEND

- Failed to detect/block
- Detected/blocking faulty
- Detected/blocking
- Detection off by default
- Detected by on-demand scan

offered the option to block it, but then failed to actually block the activity. Lavasoft was, however, the only product to detect a rather tricky attempt to replace IE as the default Windows shell in order to launch a spyware application.

eSoft's behavior-based detection was weaker than that of Lavasoft or Webroot, though it did detect and roll back an installed BHO when an on-demand scan was performed.

Alternate Data Streams

Windows machines using the popular NTFS file system support Alternate Data Streams (ADSes), a feature that allows a file to be attached to any other file or directory. Unfortunately, there's no way to detect the presence of or analyze the contents of an ADS on a standard Windows machine, making it a useful vector for malware.

For our tests, we took a specimen that an antispayware tool could normally detect and copied it into an ADS. We then used the Windows "start" command to run the malware from inside the ADS.

McAfee handled the ADS-borne spyware the best, with real-time blocking of both the malware copy into an ADS and execution from an ADS. McAfee also deleted ADS-based malware during an on-demand scan.

CA and SurfControl blocked execution of the malware from the ADS, but failed to prevent it from being copied initially. Neither cleaned up the malware with an on-demand scan using a default configuration.

Lavasoft has an option for ADS scanning, but it's turned off by default. It can provide solid real-time ADS protection, but it can only be activated at the client—there's no server-side configuration capability.

Trend Micro, Webroot and eSoft provided no protection against our ADS-borne spyware. Of particular surprise on this front was Webroot, which has a configuration option (off by default) to perform ADS scanning. When we activated this option, our ADS malware still flew under Webroot's radar. In follow-up discussions, Webroot personnel showed us how they tested for ADS spyware by using a separate program to execute malware from inside an ADS. Sure enough, when using their testing tool, the ADS malware was blocked. But, their ADS execution harness is a somewhat artificial environment, as opposed to our more real-world test using the start command. We feel that Webroot's ADS option gives users a false sense of security and therefore was worse than no protection at all, hence the lowest grade in this category.

zeroing in on price

Companies participating in our review submitted the following prices for their products.

CA

eTrust PestPatrol
Anti-Spyware 8.0
www.ca.com
\$24.80 per seat for 500-749 users for product and subscription.

eSoft (Aluria)

Desktop Anti-Spyware 1.2
www.esoft.com
\$6,250 for 500 users

Lavasoft

Ad-Aware SE Enterprise 1.7
www.lavasoft.com
\$31.25 per user for 10-25 users

McAfee

AntiSpyware Enterprise 8.5
www.mcafee.com
\$11.60 per user; \$4.96 per user subscription for 501-1,000 users

SurfControl

Enterprise Threat Shield. 3.0
www.surfcontrol.com
\$11.40 per user; \$13.97 per user subscription for 500 users

Trend Micro

Anti-Spyware Enterprise Edition 3.0
www.trendmicro.com
\$11.55 per user; \$3.47 per user subscription for 501-1,000 users

Webroot Software

Spy Sweeper Enterprise 2.5
www.webroot.com
\$8,790 for 500 users

Resilience to Attack

Increasingly, antispyware tools themselves are coming under attack by aggressive spyware that attempts to disable protection. To test resilience to these attacks, we tried to shut down each antispyware tool by shutting off its service and killing its processes at the client. We then checked to see whether antispyware protection was still functional. Many antivirus tools resist such attacks by inserting their code into other running processes, making them less likely to be subverted. None of our antispyware tools showed the resilience typical of these AV products.

SurfControl was best, maintaining protection even after its service was stopped and processes killed. McAfee also takes a strong approach: While we could shut down McAfee's service and kill its process to disable defenses, protection was automatically reactivated within five minutes, a duration that is configurable.

eSoft and Lavasoft maintained protection after their processes were killed, but died when the services were stopped. Conversely, CA kept working after the service was killed, but not when the process was terminated.

Trend Micro and Webroot were the easiest to kill, by either shutting down the service or killing the process.

Signature-based Detection

To test signature-based detection, we assembled 54 known spyware components (47 .exe files, four DLLs and three JavaScripts). We tested detection of the products in three stages:

1. We attempted to copy our spyware to a test machine to see if the product had real-time protection to prevent potential malware from being written to the file system.

2. We disabled the product, copied the spyware onto the target file system, re-enabled the product and performed an on-demand scan.

3. We copied the spyware onto a machine with the product disabled, re-enabled the product and attempted to launch each of the 47 executables to see if real-time protection followed by an on-demand scan would thwart the malware.

In analyzing our results, we looked at the overall effectiveness of each product. We awarded grades based on their ability to block spyware at each stage, placing the greatest weight on their effectiveness in stopping spyware before it had a chance to run on the system.

The clear winner in this category was McAfee, which kept us from copying 37 of the 47 executables. It found 25 of the 47 during our on-demand scan, and it left only four processes running at the end of our test series. This strong showing, which detected more than three times the number of malicious programs posted by its nearest competitor, is undoubtedly the result of its multifaceted approach to detection.

While they weren't as comprehensive as McAfee, both CA and Trend Micro performed quite well overall, each detecting 12 of the programs in the on-demand scan. Like McAfee, CA left only four processes running at the end of the testing. However, CA demonstrated no ability to block spyware from being copied to our machine.

Trend Micro, on the other hand, detected and blocked 12 of the executables we attempted to copy to the machine. But, it left a few more running processes at the end. Overall, we felt that these results balanced off, earning CA and Trend solid "Bs".

Webroot's detection rate, finding 10 of 47 specimens during the on-demand scan, was only slightly lower than CA or Trend Micro. However, the product offers no provision for blocking spyware from being copied to a computer. It left five running processes after the testing.

eSoft's decision to leave its Active Defense Shield off by default dropped it to the middle of the pack. When we enabled this shield, eSoft was able to block seven executables from being copied to the computer, matching the number it found during the on-demand scan. It also posted an impressive overall performance, leaving only four running processes when the tests were completed.

Lavasoft's lack of any real-time detection hurt its score, as it failed to block our attempts to copy spyware files to our test machine. In addition, it identified only eight of 47 executables during the on-demand scan. In the end, it left nine malicious programs running.

Finally, while SurfControl blocked six files during our attempts to copy spyware to our test machine, that's about as far as it got. It managed to detect those same six files during on-demand scanning, but failed to block or clean anything new. It left seven malicious files running.

Real-Time Detection Techniques

We were surprised by the significant variation in methods used for real-time detection. While each of the products permit an administrator to launch or schedule scans, there are significant differences in the methodology.

CA monitors the launch of executable code and blocks the execution of software that matches known signatures. Trend Micro focuses on the file system, monitoring file writes against known signatures; this is useful in detecting copy actions but not for the execution of code that sneaks onto the file system through something like an ADS. Webroot focuses its efforts toward on-

McAfee was a clear leader across the board, with solid enterprise management, strong detection and resistance to attack.

making the grade

	CA eTrust PestPatrol Anti-Spyware 8.0	eSoft (Aluria) Desktop Anti-Spyware 1.2	Lavasoft Ad-Aware SE Enterprise 1.7	McAfee AntiSpyware Enterprise 8.5	SurfControl Enterprise Threat Shield 3.0	Trend Micro Anti-Spyware Enterprise Edition 3.0	Webroot Software Spy Sweeper Enterprise 2.5
Enterprise Management/ Policy Definition and Grouping 20%	B	B-	D-	A	B-	C+	B-
Controlling Interaction with Users 15%	B-	B-	D	A	C	C	B
Reporting 15%	B	C+	D-	A	A-	B	B-
Behavior-Based Detection 15%	F	D	C	B-	F	F	C
ADS Detection 5%	B-	D-	C	A	B-	D-	F
Resilience to Attacks 5%	B-	B-	B-	B+	A-	C-	C-
Signature-Based Detection 15%	B	C+	C	A-	C-	B	B-
Real-Time Detection 10%	B	C-	C-	A	A	B-	C+
The Verdict	C+ Solid enterprise capabilities coupled with OK detection	C So-so enterprise capability and so-so detection	D+ Limited default protection and virtually non-existent enterprise capabilities	A- Solid protection across the board; excellent enterprise management capabilities	C+ Reasonably good detection; average enterprise capabilities	C Enterprise capabilities were below our expectations; average detection	C+ So-so enterprise capabilities coupled with below-average detection

demand scans in lieu of real-time protection and creates, in essence, a scheduled on-demand scan of memory for spyware signatures every five minutes.

eSoft and Lavasoft use on-demand scans as their sole detection method in their default configuration—a major limitation. eSoft depends on an administrator to activate real-time protection. When activated, eSoft's real-time defenses work much like the file system protections of Trend Micro. With no enterprise control of its real-time defenses, Lavasoft depends on users activating real-time protection, which focuses on behavior-based detection (particularly changes to the registry). McAfee and SurfControl use a blended approach that detects both file system activity and executables at launch.

Room to Improve

McAfee was a clear leader across the board, with solid enterprise management, strong detection and resistance to attack.

CA, SurfControl and Webroot were next. CA's strength lies chiefly in its relatively strong enterprise abilities, and SurfControl demonstrates reliable real-time detection mechanisms. Webroot's enterprise capabilities were just OK; its detection was below average. Very close behind were eSoft, which was OK across the board, and

Trend Micro, with average detection and somewhat disappointing management capabilities. Lavasoft, which offers a fine consumer-grade product, did not score well with its enterprise version.

Overall, the antispayware industry is far less mature than its antivirus counterpart. Most AV vendors have comprehensive detection capabilities, based largely on a combination of real-time and on-demand scan techniques. They often differentiate themselves based on user interface, software bundling, support and speed of signature releases. In the antispayware industry, on the other hand, there are major differences in each vendor's detection mechanisms (particularly behavior-based and real-time detection) and enterprise-wide management.

While enterprise spyware tools can help cut the onslaught of help desk calls, clearly most still have a long way to go. •

Contributing editor Ed Skoudis, CISSP, is cofounder of security consultancy Intelguardians, a SANS instructor and coauthor of Counter Hack Reloaded, the recently released update to his best-selling book, Counter Hack. Tom Liston is a senior security consultant with Intelguardians, coauthor of Counter Hack Reloaded and the author of a series of articles at the SANS Institute's Internet Storm Center titled "Follow the Bouncing Malware." Send your feedback on this article to feedback@infosecuritymag.com.

Reprinted with permission from Information Security Magazine, May 2006.
© 2006 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144

McAfee
Proven Security™