

# Anti-Spyware Solutions

An Independent Technology Report produced by



## Comment

### What is spyware and how do you know if it's there?

**W**hen discussing anti-spyware products, the most immediate difficulty is that there is no agreed global definition of spyware, and no agreement as to whether a given piece of malware is or is not spyware.

Compared with the firmly established classifications in fields such as macro and boot sector viruses, this does tend to make our work very difficult. How can detection be measured if the items to be detected cannot be agreed?

For West Coast Labs testing and certification purposes, the products fighting spyware are divided into three groups: gateway products, desktop products and those aiming to remove installed spyware.

Each group requires a different approach to carry out its anti-spyware functions. As for defining their opponents, we have established some base standard definitions, in which we consider that the most important facts are unauthorized usage of an Internet connection, the gathering of information (often financial or commercial) about the user and transmission of that data to external destinations.

We do not include adware in these definitions, as that produces a rather different level of problem.

This report contains an Executive Summary of the reports for each featured product. The full White Paper Test Reports are available for download at [www.westcoastlabs.org](http://www.westcoastlabs.org).

**Michael Parsons, Content Security Labs Manager, West Coast Labs**

## Introduction

### The new breed of malware that is out to make a profit by targeting your company and stealing your secrets

**O**ver recent years the history of malware can be seen as a series of waves, each cresting then fading as new waves arrive. Recently there have also been two main trends: the decline of traditional viruses and the change in the nature of malware writers. Comparatively few new pieces of malware now match the traditional definition of viruses as a parasitical infection of files and/or boot sectors. Worms remain frequent, but more and more of the new samples that continue to emerge so steadily are now loosely termed "spyware."

There is no universally agreed definition of what this term means, but two things are generally agreed. One, that most infections are now produced for commercial purposes, and two, that most of these are now written by a new breed of malware writers. Previously virus writers may have acted from malice but generally did not try to steal from those they infected. Now, malware is becoming a very profitable business.

Infection by spyware can prove very expensive. Think beyond the loss of computer service caused by old-style infections; think even beyond the theft of credit card and online banking details. What if competitors received your customer

database, your forthcoming plans, your accounts and your staff salaries? Or what if the information was stolen and you had to pay for its return?

No reliable statistics exist as to how much damage malware causes, because many companies who have found themselves compromised prefer to keep that fact hidden. Losses are estimated to be somewhere between \$50 and \$100 billion each year, with a steady increase from year to year. These include harm ascribed to viruses and worms, but increasingly they are caused by spyware.

Under the definitions that we have established, spyware includes backdoors, downloaders, password stealers, key loggers and proxies as well as programs designed to steal financial information. Our full definitions of these terms can be found at [www.westcoastlabs.org/glossary.asp](http://www.westcoastlabs.org/glossary.asp)

As to what comes next, no one can be sure. A rise in targeted attacks seems likely, where malware is not released generally but is tailored to assault a particular company for a particular purpose. Companies and individuals will need all the assistance they can get against spyware, and here the following products in this report can help.

### West Coast Labs Testing Team

All West Coast Labs tests are carried out by fully trained content and perimeter security test engineers under the direction of the CTO Jon Stearn, an acknowledged technical authority among his peers, who has over 25 years experience in the IT and security industries. Particular thanks go to Michael Parsons, Matt Garrad, Rob Tanner, Richard Thomas, Mike McMenamin and Chris Elias.

West Coast Labs Photographs Copyright  
Girls Gallaris [www.gallaris.com](http://www.gallaris.com). Art Editor:  
Sarah Lloyd, Sub-editor: Alison Welby

## Trend Micro - OfficeScan Corporate Edition

**DEVELOPER'S STATEMENT:** An integrated enterprise client security solution that delivers broad protection by incorporating core capabilities from multiple security technologies.

<b>Manufacturer</b>	Trend Micro Inc.
<b>Contact details</b>	<a href="http://www.trendmicro.com">www.trendmicro.com</a>

**O**fficeScan Corporate Edition performed without problems in the functionality tests, detecting 100% of the spyware test suite.

Trend's OfficeScan Corporate Edition (OSCE) is the corporate version of Trend's long-established OfficeScan product. It is designed to be installed centrally and then deployed to workstations, which was done easily.

The OfficeScan Management Console sits on the server and is the administrator's control panel. On the right hand side of the console it shows the various workgroups and clients on which the product has been installed, while on the left it lists a number of categories of controls. The top entry, Summary, produces a table of current clients, the status of each (online, updated, etc.) and records of current or recent outbreaks and infections.

The administrator can set options on the central server and determine whether or not to allow local users to override all or some of these settings.

OSCE includes the ability to run real-time scans against POP3 mail messages and attachments as they are downloaded from the mail server by the user, and the administrator can also enable the Virus Outbreak Monitor, which scans the network for new shared folder sessions, a high number of which can indicate viral activity.

Workstation users can run scans against drives or



folders; results are displayed locally, but also reported to the administrator. They can either download updates directly themselves or they can be enforced from the central server.

Spyware has been added to the detection capability, with only one setting that enables it to be detected (the default), or not. Again, the administrator can enforce this throughout the network.

### THE VERDICT

OfficeScan is an efficient and effective product with a well-earned reputation in malware detection. Aimed at corporate environments, it allows the administrator to maintain a high degree of control and protection over the network.



OfficeScan  
Corporate Edition  
has achieved the  
Checkmark Anti-  
Spyware Desktop  
Certification.  
[www.check-mark.com](http://www.check-mark.com)

## In the dark when it comes to choosing the right Anti-Virus, Trojan, Anti-Spyware & Firewall Solution?

### Check for the Checkmark

The Checkmark System independently tests and certifies that security products genuinely achieve internationally recognised standards. West Coast Labs' independent testing laboratories have a worldwide reputation for accuracy and reliability.

The Checkmark Systems tests products regularly to ensure that the product maintains compliance with the international standards.

If the product your using doesn't have a Checkmark, maybe you should ask why.

To find out more about the Checkmark visit our website at [www.check-mark.com](http://www.check-mark.com)



## AhnLab - SpyZero 2.0

**DEVELOPER'S STATEMENT:** AhnLab SpyZero 2.0 removes spyware, adware, trojans, keyloggers, spybots and other threats and provides a most effective system cleanup feature, boosting system performance.

<b>Manufacturer</b>	AhnLab, Inc.
<b>Contact details</b>	<a href="http://global.ahnlab.com/">http://global.ahnlab.com/</a>

**A**hnLab's SpyZero performed without any difficulty in the functionality tests, detecting all malicious spyware files in the test suite.

As a product, it is in the minority considered in this report: it is exclusively aimed at tackling spyware, with no antivirus capabilities.

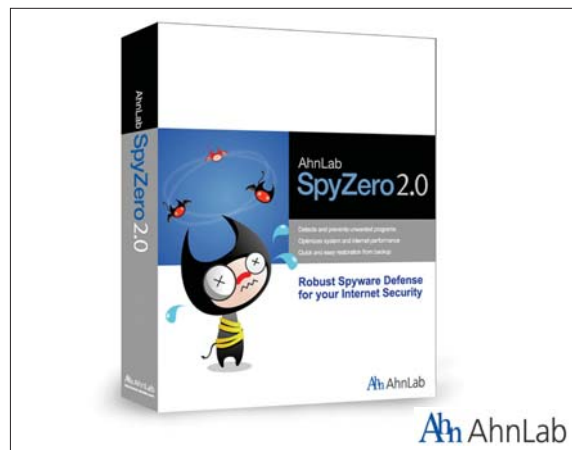
We used SpyZero as a standalone product. It installed very quickly and though the update process hung the first time while trying to contact the AhnLab server, on cancelling and restarting, it ran without problems.

The interface remains a traditional box. Three small buttons across the top are labeled Config, Update and Help. There are pages for Home, Scan and Repair, Real-Time Scan, System Cleanup, Quarantine, and Recent Activity.

Config offers the ability to password-protect settings to prevent other users modifying them, task scheduling, lists of permissible spyware and areas not to be scanned (both empty by default), and miscellaneous settings for alerting, logs and quarantine.

Most of the scans are run from the Scan and Repair screen. Each scan will search for the same preset list of malware. Items found are given a risk rating, with five rankings from Very Low to Critical. It is then possible to select some or all for 'repair'.

The Real-Time Scan can only be turned on or off;



again it is not possible to change the selection of malware to be searched for. If it is on, then ActiveX Control Blocker can also be chosen. By default both are run.

System Cleanup is a very useful facility, enabling the user to clear out 16 different repositories that are often searched by spyware looking for information.



### THE VERDICT

SpyZero, a product aimed at home users and SMEs, is an efficient product that does exactly what you'd expect of it. It is particularly suited to less technical users who can rely on its protection without needing to investigate its options.



## Equinet - NetPilot Plus

**DEVELOPER'S STATEMENT:** Equinet specialises in the manufacture of multi-functional smart unified threat management appliances that provide secure Internet access for small and medium sized enterprises. Equinet has over 30,000 of its products installed in the U.K.

<b>Manufacturer</b>	Equinet Ltd.
<b>Contact details</b>	<a href="http://www.netpilot.com">www.netpilot.com</a>

**I**n functionality testing, NetPilot Plus detected all the malicious spyware files without any difficulty while allowing innocent traffic through.

Equinet's NetPilot Plus is at heart a UTM gateway appliance, with general malware functionality for scanning email. It contains malware detection technology from Sophos (also featured in this report).



It is possible to control the device by attaching a keyboard and monitor, or, as we did, to view the console as a web page by connecting to the device across an Intranet. The web page has a clean and elegant appearance and has an increased number of options listed on the screen by adding Email Filter Policy.

Clicking each button on the left opens a new set of four to seven buttons at the top of the screen, and each of these in turn produces several options, an array of choices that might deter anyone at first sight. Fortunately the screens are well organized and easy to navigate and in most cases, the default settings are such that the administrator will not need to make any changes.

In all of this multitude of settings, there are none that directly affect the scanning for spyware. Targets cannot be allocated and the range of items being searched for


cannot be altered, being set at everything known to the engine.

This means that with the expansion of Sophos technology to include spyware in its database, NetPilot Plus has automatically added detection of spyware to its capabilities without the administrator having to take any action.



Equinet has achieved the Checkmark Anti-Spyware Gateway Certification..  
www.check-mark.com

**THE VERDICT** NetPilot Plus is well suited to satisfy the SME administrator's need for a gateway product. A detailed and clearly laid out console and wide range of available options supply all the flexibility and resilience required to protect a network.



## Aladdin Knowledge Systems - eSafe Virtual Appliance

**DEVELOPER'S STATEMENT:** eSafe's integrated content security is fast and proactive, preventing known and unknown malicious code, spam, non-productive and inappropriate content from entering your network. Its superior protection is easy to deploy and manage.

<b>Manufacturer</b>	Aladdin Knowledge Systems
<b>Contact details</b>	www.aladdin.com/esafe



In the spyware detection tests, eSafe Virtual Appliance detected all the malicious files without any difficulty while allowing innocent traffic through.

eSafe Virtual Appliance is rather unusual in that it is effectively a build-your-own device. The product comes on a boot CD, and when a machine is booted off this CD it is converted into an eSafe Virtual Appliance, which includes a Linux-based operating system. This is designed to sit at the entrance to a company's system, examining incoming and outgoing traffic.

When first installed the product is not configured, but this is a straightforward process to an experienced administrator. Once this has been done, it is then possible to connect across the intranet and open the eSafe Virtual Appliance console.


The interface will be familiar to any users of Aladdin's eSafe Gateway product – a lively and brightly colored display, topped by a grid showing what the product has seen. Adjacent to this is a pie chart concentrating on material of the particular type currently selected by the administrator, and below is a graph on which the levels of traffic from the various active protocols are shown. The graph can be scrolled backwards and forwards in time during the current running period.

The heart of the product is controlled by the Configuration section, reached via Options. Most of the

spyware parameters are shared with other areas such as antivirus, but there is one area devoted exclusively to spyware settings, offering a choice of three settings for removing ActiveX content, the ability to block access to sites known to host spyware or adware, and the blocking of known (listed) types of spyware. Each entry on the featured list appears with a brief description of its nature.

The AppliFilter is technology designed to block application level threats such as TCP/IP malicious code attacks, adware or spyware components found in "free" and commercial software and unauthorized HTTP tunneling. It provides real-time filtering of malicious Internet content entering the organization.

**THE VERDICT** eSafe Virtual Appliance is a comprehensive gateway solution. Easily understood and eye-catching graphics instantly highlight any arriving malware. Multiple options for detection and reaction exist but it can be run effectively using default options.




eAladdin has achieved the Checkmark Anti-Spyware Gateway Certification..  
www.check-mark.com

## CA, Inc - eTrust Integrated Threat Management

**DEVELOPER'S STATEMENT:** CA Integrated Threat Management combines best-of-breed eTrust PestPatrol anti-spyware with eTrust Antivirus with a single management console and increases efficiency through a common agent, logging facility, and updating tools.

<b>Manufacturer</b>	CA, Inc
<b>Contact details</b>	www.etrust.com

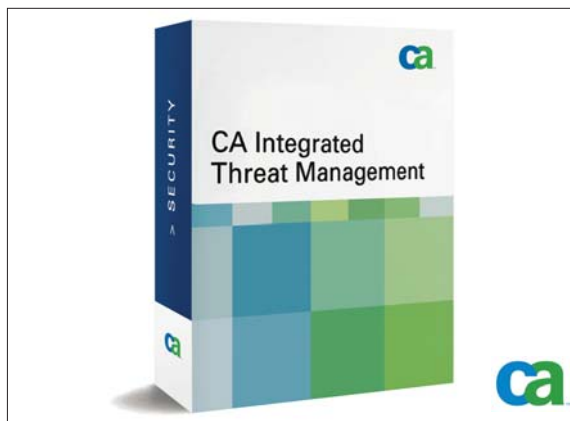
**C**A's eTrust Integrated Threat Management product completed the spyware detection tests without any problems, detecting every sample in the test suite.

In this new product, eTrust AntiVirus has now been combined with the PestPatrol anti-spyware and Secure Content Management solutions to form the new eTrust Integrated Threat Management product. This was installed and run very easily as a standalone product but can also be run in a corporate environment.

The core of the product is the console, the eTrust Threat Management Agent, with Dashboard, Scan, Settings, Update, Advanced and Logs.

Options in Settings include real-time processing, alert details and links to a management server. Active real-time processing can either affect both incoming and outgoing files or outgoing only, but not incoming only. This can seem a little odd at first sight, but is presumably so that even if infections arrive on the computer, they cannot spread and no information can be smuggled out.


Particularly useful features include Pre-Scan Block, allowing some extensions to be debarred from access to the system altogether, and Quarantine, whereby a user accessing infections over the network can be banned from the network for a given period.



PestPatrol anti-spyware functionality (apart from updates) has its own management capabilities, separate from the eTrust Threat Management Agent. It's combination with eTrust AntiVirus allows for effective detection and removal of spyware, non-viral malware, as well as annoying pests like adware to protect enterprises from unauthorized access and information theft.

THE VERDICT

eTrust ITM is an integrated threat management solution combining all the effectiveness of eTrust Antivirus and PestPatrol. All components are well designed and easy to use, making the product well suited to corporate environments of all sizes.



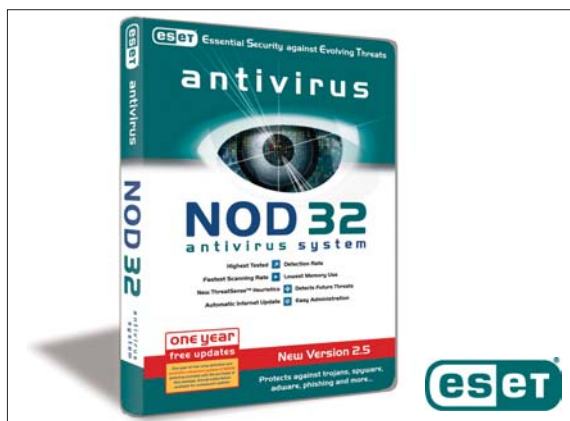

## ESET - NOD32

**DEVELOPER'S STATEMENT:** ESET protects consumers and businesses from current and evolving threats. Its award-winning NOD32 Antivirus System offers the smallest, fastest and most advanced real-time protection against viruses, spyware and phishing attacks.

<b>Manufacturer</b>	ESET
<b>Contact details</b>	www.eset.com

**N**OD32 had a 100% spyware detection capability against the test suite, performing as would be expected.

Installation of NOD32 always has been a straightforward process and remains so. Once installed, the product operates in two almost



independent parts: NOD32 and NOD32 Control Center.

NOD32 contains everything you'd expect to find for running and configuring manual scans. Heuristics are automatically used, with three possible levels of sensitivity, and advanced heuristics can also be included. Adware/Spyware/Riskware is included by default in every scan, but not potentially dangerous applications. Different responses can be set depending on where malware is found.

Once the settings have been configured to the user's satisfaction, they can be saved as profiles which can then be allocated for use in different types of scans.

NOD32 Control Center controls monitors for files (AMON), MS Office documents (DMON), MS Outlook (EMON) and the Internet (IMON). Each of the four monitors can be configured separately, and in contrast to the on-demand scanner, advanced heuristics and scanning of archives and self-extracting files are


included in the default settings, although potentially dangerous applications are still excluded.

ESET has incorporated detection of spyware into its product with a lack of ostentation. Signatures are incorporated into the main database and there is only one switch in each of the product's scans and monitors to enable or disable scanning for spyware.



NOD32 from eSet has achieved the Checkmark Anti-Spyware Desktop Certification.  
www.check-mark.com

**THE VERDICT** NOD32 has made its name successfully in the malware detection markets and has now successfully developed the technology into the spyware field. Suitable for both home and business users, it combines ease of use with good, effective results.



## Finjan - Vital Security Appliance Series NG-5000

**DEVELOPER'S STATEMENT:** This truly proactive anti-spyware solution for enterprises stops known and unknown spyware at the gateway, protecting vital business assets and intellectual property while helping to ensure privacy compliance.

<b>Manufacturer</b>	Finjan
<b>Contact details</b>	www.finjan.com

In testing the Vital Security Appliance Series, NG-5000 detected every spyware sample in the test suite in while allowing innocent traffic through.

The appliance series includes a number of differently configured devices, one of which is the VSA NG-5100. On the NG-5100 the scanner and console functions are all within the one device. It sits at the gateway between the intranet and the Internet, and can be positioned either side of a proxy.

The device came with some other products installed on it, but its antispysware code is all its own. For spyware analysis the device works on behavior rather than on signatures. For instance, behavior in network traffic can cause the installation of software to be recognized as that of spyware and banned. Exported data is also intercepted so that even if spyware makes it into the machine it cannot then transmit important information.

The device is not the easiest to configure, because of the sheer quantity of options. The default configuration among other things blocked all incoming executable files, whether malicious or innocent, and we discussed our needs with the (very helpful) company before settling on the final configuration.

The heart of the product can be found on the console in the first of seven categories, Policies. Default and



emergency policies (the latter blocking everything not previously whitelisted) are already set, and copious options are available.

This is a thoughtfully developed, well structured product. Everything is clearly laid out and default settings will normally prove to be acceptable for spyware detection requirements.

**THE VERDICT** Finjan's Vital Security Appliance Series NG-5100 is a versatile and detailed gateway behaviour-based device for SMEs. Easy to master, it allows the administrator a very easy route to identify and adapt settings as required to protect the network.




Vital Security Appliance Series NG-5000 has achieved the Checkmark Anti-Spyware Gateway Certification.  
www.check-mark.com

## Internet Security Systems - Proventia Desktop

**DEVELOPER'S STATEMENT:** A unique multi-layered approach combines patent-pending behavioral, vulnerability-centric, and signature-based technologies to provide proactive protection against current and newly discovered network and malware threats.

<b>Manufacturer</b>	Internet Security Systems
<b>Contact details</b>	www.iss.net

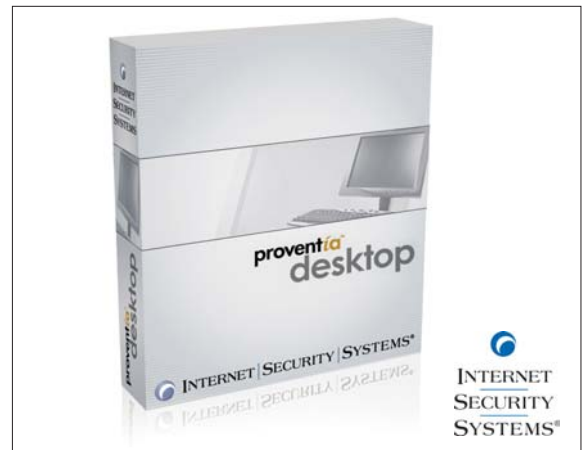
All functionality tests for spyware detection were carried out by Proventia Desktop without problems detecting 100% of the samples.

ISS's Proventia Desktop is part of ISS' suite of products, Proventia Enterprise Security Platform, and installs as a standalone product. It is without on-demand scanning abilities and operates solely as a real-time scanner.

Any changes required are made using five buttons across the top, in particular Tools. There are eleven divisions of settings, enabling, among other features, selection of one of four levels of protection against unsolicited inbound traffic, exclusion of certain items from monitoring, and buffer overflow exploit prevention, covering a predefined but configurable list of commonly attacked files.

One of the eleven areas is Application Control, which blocks spyware as defined in the X-force Database, ISS's collection of the threats and vulnerabilities on which much spyware depends. Spyware definitions are added to this and updates automatically rolled out.

Proventia Desktop offers pre-emptive action to prevent spyware infections, stopping infections before they can cause any threat to information or outages while repairs are undertaken, but it does not include any removal facilities should any infections have occurred



before installation. It should however be able to disable any installed spyware and prevent it from threatening the machine's security.

The product is very easy to run because it makes so little demand upon the user and is an effective solution which can be used as part of a larger suite of products for higher levels of security across the network.



Proventia Desktop has achieved the Checkmark Anti-Spyware Desktop Certification. [www.check-mark.com](http://www.check-mark.com)

### THE VERDICT

Proventia Desktop is an easily run and effective product, intercepting incipient spyware infections and blocking existing infections from working. Part of a suite aimed at corporate customers, its' real-time scanner makes few demands upon the user.



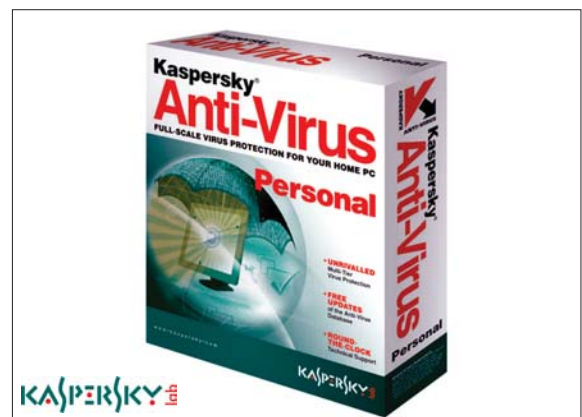
## Kaspersky AntiVirus Personal

**DEVELOPER'S STATEMENT:** Kaspersky Anti-Virus Personal is designed to provide protection from all kinds of malicious software like viruses, worms, trojans, hacking tools and spyware for home computers running Windows.

<b>Manufacturer</b>	Kaspersky Labs
<b>Contact details</b>	www.kaspersky.com/personal

Kaspersky AntiVirus Personal (KAV) had no problems with the spyware detection functionality tests with a 100% success rate.

KAV installed very easily and uneventfully. Updating also ran smoothly. Users should note that the product has two types of database: Standard, with definitions



for viruses, worms, Trojans, hacktools and spyware; and Extended, which adds adware, riskware and dialers.

The default is the standard database. It is not immediately obvious how to make the change and the user is not alerted as to which database is in use.

However, the extended database is implemented by making a change in Settings, under Threats and Exclusions. Sensibly, the user is warned that its implementation may lead to the detection of important programs as infected so the response to an infection should be changed to consult the user rather than automatic deletion or quarantine.

Real-time protection can be set to one of three levels, the default (Recommended) being a compromise between speed and thoroughness. On-demand scanning also has the same three settings.

Spyware detection has been incorporated into KAV

with a minimum of fuss. The standard database entries will detect many pieces of spyware, but the extended database is needed for optimum detection.

KAV is a very easy product to use. It can be run on default settings without any major insecurities, apart from the desirable change to the database.



Anti-Spyware DESKTOP

Kaspersky AntiVirus Personal has achieved the Checkmark Anti-Spyware Desktop Certification. www.check-mark.com

**THE VERDICT**

Kaspersky AntiVirus has a well-deserved reputation in the antivirus and Trojan fields and merits a similar reputation in spyware. This Personal edition is for the home user and provides copious assistance to the user, making it particularly suited to less technical purchasers.



## VirusScan Enterprise with McAfee AntiSpyware

**DEVELOPER'S STATEMENT:** McAfee AntiSpyware Enterprise, the leading enterprise-class anti-spyware software solution, uses true On-Access scanning to identify, proactively block, and safely eliminate potentially unwanted programs (PUPs) for optimal business availability.

<b>Manufacturer</b>	McAfee, Inc.
<b>Contact details</b>	<a href="http://www.mcafee.com/us/products">www.mcafee.com/us/products</a>

**V**irusScan Enterprise performed without difficulty in the detection tests, correctly dealing with 100% of the spyware samples in the test suite.

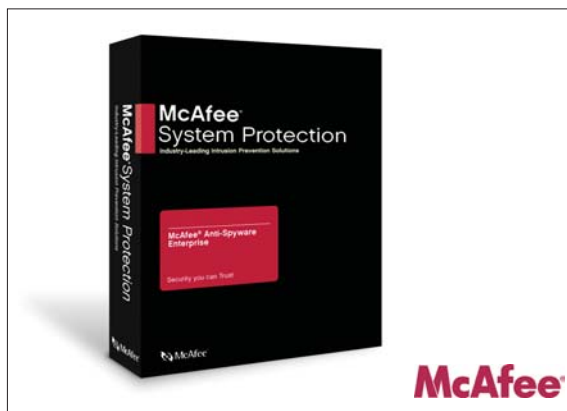
The McAfee AntiSpyware Enterprise (MAS) module is a separate attachment to McAfee's VirusScan Enterprise (VSE) which requires VSE to have been previously installed. In addition, the version numbers for both VSE and MAS must match for the module to work properly.

The products are installed separately and both installations passed off without problems.

Access Protection is used to block incoming or outgoing network traffic for specified ports, and can thus disrupt the running of many pieces of spyware such as backdoors and downloaders.

The most important part of the antispyware defences, however, is the Unwanted Programs Policy, which lists seven categories of undesirable programs that can be selected for detection. VSE's default is not to select any, while the installation of MAS changes this to select all entries. If some or all of these categories are selected when VSE but not MAS is installed, VSE can use the shared definitions file to detect a number of pieces of malware, but MAS will achieve significantly better results.

Scan All Fixed Disks and each on-demand scan, whether created before or after the installation of MAS,



will consult the current list, take its instructions as to what to detect from the categories selected therein, then use MAS to detect known and heuristic samples falling into those categories. While each scan task can treat detected items in different ways, it is not possible to have multiple scans with different choices from the list – a change in the list is automatically reflected in all tasks.

**THE VERDICT**

VirusScan Enterprise, the corporate version of the well-known antivirus product, has now added the McAfee AntiSpyware Enterprise module and comfortably adapted to the battle against spyware. This tried and tested product remains efficient, effective and easy to use.



Anti-Spyware DESKTOP

VirusScan Enterprise has achieved the Checkmark Anti-Spyware Desktop Certification. www.check-mark.com

## Panda - ClientShield with TruPrevent Technologies

**DEVELOPER'S STATEMENT:** Panda ClientShield with TruPrevent Technologies is a global security solution for workstations in network environments, which protects against viruses, spyware, hackers, spam and other known and unknown threats.

<b>Manufacturer</b>	Panda Software
<b>Contact details</b>	<a href="http://www.pandasoftware.com/products">www.pandasoftware.com/products</a>

**C**lientShield had no problem with the spyware detection tests, achieving a 100% against the test suite.

Panda Software's ClientShield is a component of its AdminSecure product, and consists of a number of modules. AntiVirus now includes settings (Files and Mail) for spyware and other categories of malware, and it was the only module used here.

A window at the bottom of the AdminSecure interface tells the administrator which modules have been installed on a selected workstation and whether or not they are active and up-to-date. In addition, the administrator controls the settings used by the user's scans and by the installed modules.

Available settings for Files include the ability to search for four specified types of malware: spyware, malicious dialers, jokes and hacking tools. All are selected by default. Only files with one of a list of extensions (which can be amended) are scanned, but the list is fairly inclusive in range. Interestingly, heuristics are not enabled by default, although there are three levels from which to select if they are to be used.

Mail looks at incoming mail, with default settings including the use of heuristics, but not the scanning of Outlook Express. Default scanning does not look for private data theft or for phishing. It does search for all




other forms of malware as listed above, plus hoaxes, but scans only a list of specified extensions and does not include files with no extensions. Again, this can be altered.

Panda's addition of anti-spyware detection has caused little change in the product; indeed, users cannot tell whether or not it is being detected. The same signature files update all malware definitions.

THE VERDICT

This product, with its well-earned reputation earned in malware detection technology, is suited to companies of any size. The administrator controls the product settings, ensuring that the systems are efficiently protected against a variety of spyware threats.




*ClientShield with TruPrevent Technologies has achieved the Checkmark Anti-Spyware Desktop Certification.*  
[www.check-mark.com](http://www.check-mark.com)

## Softwin - BitDefender 9 Antispyware

**DEVELOPER'S STATEMENT:** BitDefender Antispyware monitors your computer and prevents potential spyware threats in real time, before they can do damage. It prevents loss or theft of data, and productivity losses due to spyware infections.

<b>Manufacturer</b>	Softwin
<b>Contact details</b>	<a href="http://www.bitdefender.com">www.bitdefender.com</a>

**B**itDefender 9 correctly detected all spyware samples in the test suite. Softwin has aimed this product at the home user, in particular at the family connected to the Internet who want both security and parental control over their children's activities. As a result, the product is designed to be, and is, very easy



to install and configure. The comparatively inexperienced target market does not affect the technical quality of the product.

The AntiSpyware module of BitDefender has six sections: Shield, Scan, Scheduler, System Info, Quarantine and Report. Shield is the on-access protection against spyware, which includes separate facilities for files, dial, script, cookies and registry. Dial allows the user to prevent applications from making telephone calls. Cookies and scripts can be accepted or rejected on a domain basis or universally, though this is not activated under default settings.

Scan provides on-demand protection, with two general settings – Quick and Deep. Quick scans important system settings and running programs, while Deep will also scan the contents of drive(s) or folder(s) specified by the user. By default scans will use heuristics, and will detect incomplete virus bodies.


Suspicious files detected in these ways can be sent automatically to the BitDefender Labs.

BitDefender can safely be run on default settings to provide a secure working environment, but can also be configured by those with a little more expertise to achieve first-class tailored protection.



BitDefender 9 Internet Security has achieved the Checkmark Anti-Spyware Desktop Certification. www.check-mark.com

**THE VERDICT** BitDefender 9 Internet Security has been carefully considered and designed for the needs of a home or small office. Its comprehensive malware protection and additional facilities are particularly suitable where multiple users share one workstation.



## Sophos Anti-Virus

**DEVELOPER'S STATEMENT:** Sophos Anti-Virus provides best-of-breed antivirus protection for enterprise IT environments. Sophos Anti-Virus ensures file servers, desktops and laptops remain free from viruses, Trojans, worms and spyware.

<b>Manufacturer</b>	Sophos
<b>Contact details</b>	www.sophos.com

**S**ophos Anti-Virus performed without difficulty in the tests, detecting 100% of samples in the spyware test suite.

Sophos released Sophos Anti-Virus version 5 in 2005, and the product has undergone a number of changes in this upgrade.

The installation remains as easy as ever and the changes appear when the interface is displayed. An HTML display now appears, with a clear and attractive display information.

The main part of the display features four permanent entries: Scan local disks, Set up a new scan, Manage quarantine items, and Configure Sophos Anti-Virus, as well as, in a lower section, any new scans created by the user.

Updating is now done automatically, with hourly checks for new information. This time interval can be altered either by clicking on the icon in the lower right corner, or by entering Configuration.

Interestingly, a new scan can be run or modified only by the user who created it, and scheduling a scan requires the password of the user to be entered. This could be an extra security feature, but it could also lead to duplication of effort.


Sophos has taken a very simple line in the incorporation of anti-spyware features into their product



– there is no apparent difference whatsoever. Spyware definitions have been quietly added to the database, and the engine now automatically searches for spyware along with its previous malware targets.

The user will want to investigate some of the default settings but that done, Sophos Anti-Virus remains simple to use and efficient at its job; it has expanded into its new function with ease and success.

**THE VERDICT** Sophos Anti-Virus is a familiar name in the anti-malware market, appropriate for both home and corporate users. Its unobtrusive addition of spyware detection capability to its targets has been carried out thoroughly and effectively.




Sophos Anti-Virus has achieved the Checkmark Anti-Spyware Desktop Certification. www.check-mark.com

# Webroot - SpySweeper Enterprise

**DEVELOPER'S STATEMENT:** Webroot Spy Sweeper Enterprise is a centrally managed, scalable enterprise solution that provides best of breed protection against malicious spyware, adware, and other intruders.

<b>Manufacturer</b>	Webroot
<b>Contact details</b>	<a href="http://www.webroot.com">www.webroot.com</a>

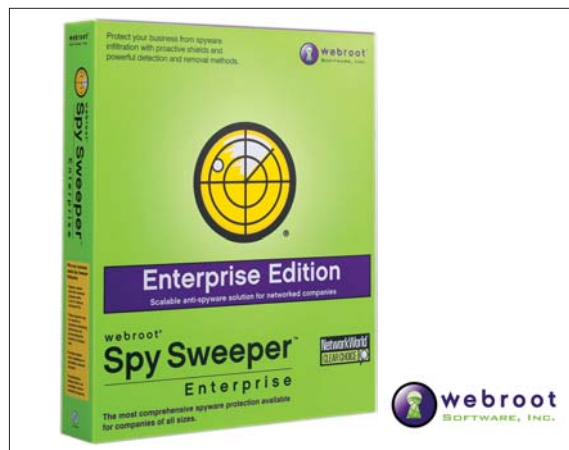
**S**pySweeper Enterprise performed without any difficulty in the functionality tests, dealing effectively with a variety of installed spyware samples on the test network.

This product deliberately concentrates its main efforts on the identification and removal of spyware already on the system.

A Dashboard is displayed when the console opens, giving a quick overview of the system's health. A more detailed set of subscreens show how many and which of the controlled desktops fall into moderate or critical problem areas. It also includes the company's list of top spyware threats for the last two days.

Manage Desktop Applications is the area where configuration of detection is carried out. By default none of the 16 Smart Shields are activated, a rather unexpected setting. The default areas for scanning are memory, registers and all folders and an alternative choice is known spyware folders only. The editing of many options can individually be permitted or prohibited.

The product deploys without difficulty, and in this case we were deploying it to systems already infected with spyware, the infections were dealt with effectively. Scanning reports indicate the name of the spyware found and the number of traces of that particular piece of spyware found, so that you might find a total of 17




traces of 3 infections, each trace referring to a different file or registry setting. The user is shown full details of each trace of infection after the scan, but the console logs provide rather less information.

The product proved to be very thorough in its detection, locating every trace of infection on the various machines to which it was deployed.

THE VERDICT

SpySweeper Enterprise is designed and developed for the corporate market. It is both scalable and thorough in its identification of installed spyware on workstations, making it a very good solution for dealing effectively with spyware infections.




**Anti-Spyware INSTALLED**


*Webroot as achieved the Checkmark Anti-Spyware Installed Certification.*

[www.check-mark.com](http://www.check-mark.com)



## Product Testing, Evaluation and Certification Services

### West Coast Labs Services

- Advanced product testing and validation
- Product feature and performance analysis
- Product-design review and development
- Marketing your technology message to a global buying market
- Beta testing and evaluation
- Custom testing 
- Certification

For full details of West Coast Labs' product testing, evaluation and certification services contact Mark Thomas, Sales Manager: [mthomas@westcoast.com](mailto:mthomas@westcoast.com)

