

THE TECHNOLOGY REPORT - JANUARY 2005

Anti-Virus and Trojan desktop solutions



www.westcoastlabs.org

In the dark when it comes to choosing the right Anti Virus, Firewall and VPN solutions? 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 System tests products regularly, in some cases as frequently as every six weeks, to ensure that the product maintains compliance with the international standards.

If the product you're using doesn't have one, maybe you should ask why.

To find out more about the Checkmark visit our web site at www.check-mark.com

The following companies have products tested and certified under the Checkmark system:

**AhnLab • Aladdin • Alcatel • Appgate • Blackspider • Cat • Command • Computer Associates • Cybersoft
Equinet • Eset • F-Secure • GFI • Hauri • Inty • Kaspersky • McAfee • MicroWorld • Norman • Panda
Preventon • SecurePipe • Softwin • Sophos • Stonesoft • Symantec • Trend Micro • ViGuard • VirusBuster • Wanadoo**

Comment

Security professionals need real-world product testing with objective reports



Welcome to the first in West Coast Labs' series of annual Technology Reports. There are five more planned for 2005, covering technology areas such as anti-virus firewalls, anti spyware, anti-spam and vulner-

ability assessment.

More are planned for 2006, and beyond. We anticipate that this program will rapidly become a key point of reference in the purchasing cycle for security professionals around the world, enabling them to confirm that the products they choose are at the cutting edge of security technology – and right for their business.

Each Technology Report module will feature an independent technical analysis of the functionality and performance of a number of the world's leading products in specific technology sectors. Participating products are tested to pre-published methodologies and reviewed against the functionality criteria of the Checkmark certification program. We also carry out additional tests to establish how products perform in simulated business environments that reflect real-world situations. The test criteria for each report is available online at www.westcoastlabs.org.

While this first publication only contains an executive summary of 14 participating products, full results can be found in the White Paper test reports available for download at www.westcoastlabs.org.

Each White Paper contains a complete Features and Functionality Buyers Guide, which looks at over 30 different product features. You can also download trial versions of the tested software.

Throughout this program, our aim is to provide you with objective reports and comment that will enable you to choose the right products for your organization. We welcome your feedback. avfeedback@westcoast.com

Jon Stearn
CTO, West Coast Labs

Introduction

Is desktop AV protection still important for the security of corporate environments?

The battle between virus writers and the anti-virus products has raged unabated during 2004. California based Computer Economics, Inc. estimates that worldwide losses due to viruses in 2003 reached \$13bn. In 2004 it estimates that the cost rose to \$116.7bn overall. In October 2004, MessageLabs noted that of the over 2.29 billion emails they processed, one message in every 32.24 contained a virus.

Significantly, just four families of viruses in 2004 have, according to Computer Economics, had a worldwide impact of a staggering \$11.5bn. Those families of viruses were the prolific, ever-changing MyDoom, Bagel and NetSky, and the Sasser worm. Sasser began spreading widely on May 1, 2004, exploiting a vulnerability in a component of the Windows operating system within 17 days of Microsoft announcing a patch.

Malware motivation

Viruses, worms and Trojans are the main elements of malware that anti-virus software aims to detect, repair or delete. Many anti-virus products also include anti-spam functions. Although often referred to generically as viruses (including in this article), the three types of malware have different properties and pose different risks.

Worms such as Sasser spread by sending exact (or near exact) copies of themselves to other email addresses found in an infected system's address book, whereas viruses propagate by hijacking other files. Both use email as a delivery mechanism but can also use web sites, IRC, instant messaging and peer-to-peer (P2P) services, where they exploit vulnerabilities (such as buffer overruns) in software installed on the target machine. Trojans are programs that are, like the Trojan horse, loaded on to a system by stealth or subterfuge. They can operate unseen as mail servers or to steal information from the target computer, or to launch denial-of-service (DoS) attacks.

The profile of the virus writer is changing says Ed Skoudis of International Network Services and a certified SANS instructor. "Computer exploit and malware developers have numerous

Introduction continued...

motivations. Some are hobbyists, just looking to have fun while pushing the envelope. Many others are researchers, working at universities, vendors, and consultancies, all trying to understand new attack vectors to help improve our defenses. But a handful are purely evil, wanting to cause serious damage to their intended targets or enjoy a perverse thrill associated with hurting lots of people with some nasty code.”

Commercial exploits

As computer users get more virus aware, virus writers are using social engineering techniques to persuade them to open an attachment or follow a URL. Around the U.S. election in early November 2004, the W32/Famus.F worm sought to persuade recipients that a message from Osama bin Laden was being forwarded in the attached file.

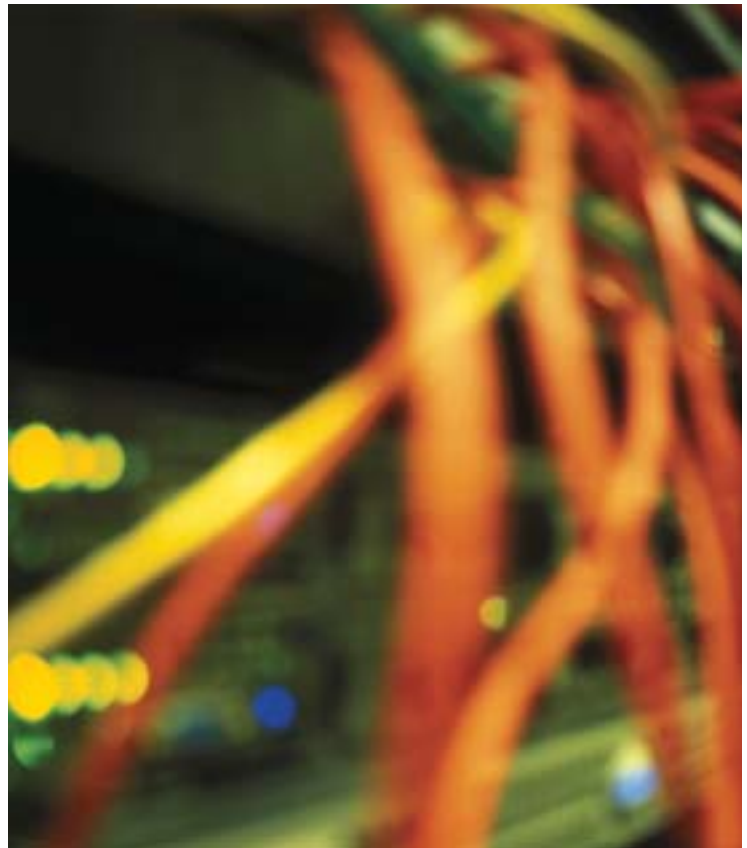
There is no doubt that many virus exploits are now commercial in their intent. MessageLabs, in their October 2004 monthly report, chronicled ‘The Rise of the Zombie Botnets’ – not a new horror film but an all-too-real problem for security professionals. They report that “since early 2003, a common device for deploying a Trojan backdoor component has been the staged technique.”

Initially, the virus would initiate the download of a second stage from a main website called a mothership. When this was overcome by closing down the mothership, newer viruses such as Bofra (first seen in autumn, 2004) use an HTTP link to another infected site in order to download a second or third stage payload. MessageLabs also report that “approximately 70 percent of the spam intercepted over the past 12 months has been sent through zombie botnets.”

Guard your desktop

As corporate networks secure themselves more effectively at the perimeter, does that move desktop anti-virus down to the smaller end of the market? Probably not, since all businesses need critical security elements which include anti-virus at all layers from the perimeter to the desktop. With the rise of instant messaging and P2P in corporate environments, and in the use of removable memory devices, protecting the desktop is still as important now as it was before the internet arrived.

With the likes of MyDoom, Bagel, NetSky and Sasser having such a staggering cost impact on



businesses, it's vital to ensure that your desktop solution is at the cutting edge of dealing with these malevolent threats. There are 14 AV solutions featured in this Technology Report, each of them tested against these viruses and many of their variants – which are included in the virus detection functionality tests.

Test specifications for the AV and Trojan desktop solutions

The overall objective has been to evaluate each AV product in a controlled environment over a two- to three-month period. Throughout this period each product had internet access and was configured as recommended to update online.

Products were tested in accordance with the functionality criteria of the levels of registration they hold in the Checkmark AV certification program. Each product report addresses four specific areas: management/administration, functionality, and performance, plus additional feature testing.

Full details of the test specifications and the criteria against which each of the products were tested can be found online at www.westcoastlabs.org in the Technology Report section.

V3 Pro VirusBlock 2005 for Windows XP Pro

DEVELOPER'S STATEMENT: Focuses on users in the high-speed internet environment. Whether in business or home, it will give seamless protection for everyday threats.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: V3 Pro VirusBlock 2005 for Windows XP Pro
Manufacturer: AhnLab
Contact details: <http://info.ahnlab.com/english>
Full White Paper: www.westcoastlabs.org

The product installed easily and was updated online. Automatic updates can be scheduled, and updates can also be downloaded and applied manually. The user is informed if virus definitions are out-of-date. The product also automatically includes AhnLab Personal Firewall 2004.

The GUI presents a clean and efficient appearance. A column on the left allows the user to tab between the anti-virus facilities and the firewall, while on the anti-virus page a further series of pages are offered which include system scanning, event and scan logs, and quarantine. Buttons above lead to update, configuration, refresh and help. There is also a Security Warning Report page for analyzing system weaknesses and indicating the patches that can block them. The Home page displays a useful summary of the main settings in use on the real-time scanner.

Scanning and configuration

On the System Scan page the various scanning targets are displayed for the user to choose what should be scanned. These can be easily selected through a simple expandable directory tree structure.

Options available to the user upon detection of a virus, both on access and on demand, are Delete, Repair or Do Nothing. Items in quarantine can be restored to their original position, reported to AhnLab, saved in a temporary folder, or simply deleted.

The Event Log displays, as one would expect, all occurrences on the system, such as updates, and the start and stop of scans. The Scan Log lists in a table all the infections found during scans. Each entry when clicked on shows all the details in a box on the screen, though a minor drawback is that the box cannot be extended if the entry runs beyond the displayed area, for example, where there is a long directory name.

Configuration offers three preset protection levels (high, medium or low security) and one



that can be customized to suit the user's needs. Default options include scanning of emails and anti-spam protection. One useful feature is that warning emails are not normally sent to the 'senders' of infected emails – with so many addresses spoofed nowadays, the likelihood that the warning will reach the original sender is increasingly slight.

Help files are on the hard disk and a virus encyclopedia is online.

Detecting and disinfecting

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files once it had updated definition files. Similarly, it had no problems dealing with the pre-infected systems.

In the compressed file tests, only six files out of the 18 were detected as infected. The product did not mention that six of the files were encrypted. It did detect all the Trojans in the West Coast Labs collection.

THE VERDICT

V3 VirusBlock 2005 seems well suited to an individual or smaller office and could also be useful in larger organizations. The solution has very fast scanning times which were impressive, as was good detection of viruses and trojans.



eTrust Antivirus 7.1.1 for Windows XP Pro

DEVELOPER'S STATEMENT: SME to enterprise customers get complete virus protection from the perimeter to the PDA, with flexible reporting, for one price.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: eTrust Antivirus 7.1.1 for Windows XP Pro
Manufacturer: Computer Associates Inc.
Contact details: www.ca.com
Full White Paper: www.westcoastlabs.org

The product was installed and tested in standalone mode. Installation was straightforward and the product was updated manually with downloaded updates. New updates appear daily, more often in outbreaks, and automatic updates can be scheduled. The user is warned if the product has not been updated, and in a corporate set-up updates can be distributed.

The product contains two scanning engines: CAI's traditional product Inoculate, and another longstanding product later bought by CAI, Vet. We tested the Inoculate engine. eTrust also offers two methods of scanning: secure and thorough. We used the default setting, secure.

eTrust at work

The GUI is clear and uncluttered. Four buttons run across the top: File, Scanner, View and Help. The View button is used to switch between two screens, the first showing the scanning targets and the second showing the logs available. On the first screen, the various scanning targets are displayed for the user to choose what should be scanned. An area at the bottom shows details of infected files found in the last scan.

The File button offers printing facilities and the Help button includes a link to an online virus encyclopedia. The Scanner button is the main area of activity, leading to configuration of the local and real-time scanners, scheduling of jobs, user notifications (which can be turned off or sent to a remote address), the update process, and virus submission facilities.

Both local and real-time scanners have the ability to cure or disinfect (the default), delete, rename, move or merely report on an infected file. If the file cannot be disinfected the options available are Move, Rename or No Action (the default). The two scanners can be configured separately.

On the log screen the various different logs are divided by type, each type showing a separate list of the reports of that type that are available.



Logs can be printed or saved in a file, either partially or wholly.

eTrust detected all 372 viruses in the first test once updated definitions had been given, and disinfected the appropriate files.

Dealing with the problems

With the pre-infected systems, those infected with W32/Korgo.A and W32/Netsky.Z were disinfected without problems. Four reboots of the system infected with W32/Lovgate.Z were required before it was completely disinfected but this was finally achieved.

eTrust will normally consider a file by looking at its extension, but also has the capacity to examine a compressed file and determine its nature from its analysis. Using the latter method, it detected ten out of the 18 compressed files as infected and reported six as encrypted.

For the Trojans, eTrust disinfected the appropriate files without problems.

THE VERDICT

eTrust Antivirus performed very well in testing, detecting and disinfecting as expected. It is a reliable, effective AV solution that is worthy of serious consideration, particularly for corporate customers, who will find the extensive reporting facilities of most use.



Command AntiVirus Pro 4.92.1 for Windows XP

DEVELOPER'S STATEMENT: Command Antivirus targets small and medium businesses, enterprise corporate, education, government, ISPs, and single users.



Anti-Virus
Level 1



Anti-Virus
Level 2

Product: Command AntiVirus Pro 4.92.1 for Windows XP
Manufacturer: Authentium
Contact details: www.authentium.com
Full White Paper: www.westcoastlabs.org

Based on the F-Prot Professional scanning engine, which has been developed over a period of more than twelve years, Command AntiVirus includes a mix of heuristic and signature-based detection methods.

The product installed in a straightforward manner. It features a number of preset tasks for scanning processes, each of which has its own individual settings.

The default action of the product on detecting a virus is to disinfect the file, with options to report only, quarantine and delete. Clear and detailed information is provided in the logs, including precise virus names rather than the generic descriptions more common nowadays.

User notifications can be disabled if required – as a standalone product, there are no remote notifications available. The product can scan inside archived files, i.e. zipped or packed files (frequently used for transmitting or storing data) in which the pattern of an infected file will be distorted, but this is not the default setting.

Scanning is by default on a given list of file extensions, which can be modified. A real-time



scanner, Dynamic Virus Protection (DVP), can be configured to suit users' needs, or disabled.

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files.

THE VERDICT

Reliable and comparatively fast detection are Command's established trademarks. Some configuration is advisable in areas such as compressed files to obtain the best results. Don't overlook this product in any business environment.



Quick Heal XGEN 7.2 for Windows XP Pro



DEVELOPER'S STATEMENT: Anti-virus product specially designed for home and SOHO users. Best suited for protection against internet threats.



Anti-Virus
Level 1

Product: Quick Heal XGEN 7.2 for Windows XP Pro
Manufacturer: Cat Computer Services Pvt. Ltd.
Contact details: www.quickheal.com
Full White Paper: www.westcoastlabs.org

Quick Heal installed without any difficulty. The GUI is a little subdued in appearance, but provides uncomplicated, easy-to-navigate menus. Scanning is by folder or by drive, with incoming email scanned by default.

Quick Heal detected all 372 viruses in the test suite once updated definitions had been applied.

In the tests on compressed files, eight files out of the 18 were detected as having infections. No files were labelled as encrypted or incapable of being scanned.

The product delivered some of the fastest scanning times.

THE VERDICT

Quick Heal provides an ideal solution for home and SOHO users, who want comprehensive protection but do not want to be overburdened with complex configuration options.



Kaspersky Anti-Virus Personal 5.0

DEVELOPER STATEMENT: Easy-to-use protection for home PCs. Destroys threats at all entry points to your PC, including email, internet and removable media.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: Kaspersky Anti-Virus Personal 5.0
Manufacturer: Kaspersky Labs
Contact details: www.kaspersky.com/personal
Full White Paper: www.westcoastlabs.org

Kaspersky Anti-Virus installed in a straightforward manner. It is updated online, and manual updates can also be downloaded. New updates are produced at least daily, more frequently during outbreaks, and are made available to all customers. Automatic updates can be scheduled and the user is informed of out-of-date definitions.

The GUI is easy to use, offering three pages: protection, settings and support. The first two scan and configure respectively. Support is for accessories such as help and links to internet-based services.

Working on clean-up

At first it appears that only drives can be scanned and not individual folders, but it is possible to add folders to the list of scan objects. When infected items are found the scanner can ask what action it should take, and it is possible (but not compulsory) to apply that action to all such infections found in that scan. Infected files are backed up to a special storage area before repair to ensure that any problems encountered during disinfection will not be irrecoverable.

Both the scanner and the real-time scanner come with the same three levels of settings: maximum protection, recommended and high speed, the default being recommended.

If any problems are encountered, there is a helpful troubleshooting guide on the hard disk. Additional support and a virus encyclopedia can be found on the internet, and it is possible to send a sample to Kaspersky Labs via email.

Each scan produces an individual log in three sections: statistics, results and settings used. Unscannable files are reported. Logs can be produced, sorted and saved into files, but it is not possible for the user to specify which information will appear in the log. They are normally deleted after 30 days.

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files.



With the pre-infected systems, it removed the infections of W32/Korgo.A and W32/Netsky.Z. When installed on the system infected with W32/Lovgate.Z, it produced a replica computer game with a box for each infected file, challenging the user to click on as many boxes as possible before a 60-second shutdown period expired. This 'game' was repeated after restarting the computer for those files not disinfected in the previous session, and the infection was eventually removed.

Penetrating the layers

Kaspersky has recently expanded its detection of packed and archived files and this test posed them no problems. The six encrypted files were reported as being encrypted with a password, and the password was requested in order that the files might be scanned. The others were all detected.

The product also detected all the Trojans in the West Coast Labs collection.

THE VERDICT

Kaspersky Anti-Virus is based on a scanning engine that is among the best in the anti-virus industry. It performed very well in all our testing, and was one of the few that identified all virus samples in very deeply nested zipped files, logging those encrypted and password protected.



McAfee VirusScan Enterprise 8.0i for Windows 2000 Pro

DEVELOPER'S STATEMENT: Advanced, proactive protection for desktops and servers. The solution contains anti-virus, HIPS and firewalls protection from known and unknown attacks.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

| | |
|--------------------------|------------------------------------------------------------------|
| Product: | McAfee VirusScan Enterprise 8.0i for Windows 2000 Pro |
| Manufacturer: | McAfee, Inc. |
| Contact details: | www.mcafee.com |
| Full White Paper: | www.westcoastlabs.org |

VirusScan Enterprise installed without any problems and was easily updated. Updates can be downloaded and applied manually or automatically. It is possible to get separate updates for engine and databases, or have both incorporated into Superdat files. These are released weekly, but more frequent updates are available during emergencies, and the computer can automatically download the latest update at start up. In a corporate set-up it is possible to distribute updates.

Beyond detection

The design of the GUI has remained unchanged for some time, but the tasks have been considerably altered in the upgrade from version 7 to version 8. VirusScan now includes buffer overflow detection, unwanted programs policy and access protection (port-blocking rules).

Access protection enables the user to block traffic through ports, so that it becomes possible to disable those viruses trying to infect the computer across the internet or another network. Many such viruses are coded to use a particular port and will either not infect or be ineffective if that port is unavailable.

Unwanted programs policy enables the user to expand detection beyond viruses, while buffer overflow detection prevents the execution of arbitrary code on the machine, another favored tool of virus writers.

The product features all the standard tasks that the user would expect to be available, such as scanning the hard disk, scanning email (incoming by default), and updating. A panel at the top offers menus to other utilities such as configuring the real-time scanner, the Error Reporting Service that will monitor and report errors in the product installation, and an option to repair the product installation.

Technical support and a virus encyclopedia are available on the internet, and samples of suspicious files can be submitted via a link in the menu.



Each task type has its own log and highlighting a task and choosing View Log shows all entries for that type of task. All or part of a log can be printed off or saved in a file.

Cleansing and configuring

Configuration can take place remotely and local users can be prevented from changing settings (e.g. disabling the real-time scanner) unless a password is entered. At shutdown the floppy disk drive is checked to deter booting off an infected disk.

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files. The solution also disinfected the previously infected systems without problems. Where the compressed files were concerned, once scanning of archive files was enabled, 12 viruses were detected and six files were reported as being encrypted.

Finally, VirusScan detected all the Trojans in the West Coast Labs collection without problems.

THE VERDICT

McAfee VirusScan Enterprise performed very well in testing, though the option to scan zipped files must be enabled. It then detected all files in unencrypted archives, no matter how deeply nested, and clearly identified and logged those encrypted. Worthy of serious consideration for all enterprises.



F-Secure Anti-Virus Client Security for Windows XP Pro

DEVELOPER'S STATEMENT: Complete protection against malware, hacking, spyware and spam. The company's key strength is its industry-leading speed of response to threats.



Anti-Virus
Level 1



Anti-Virus
Level 2

Product: F-Secure Anti-Virus Client Security for Windows XP Pro
Manufacturer: F-Secure
Contact details: www.f-secure.com
Full White Paper: www.westcoastlabs.org

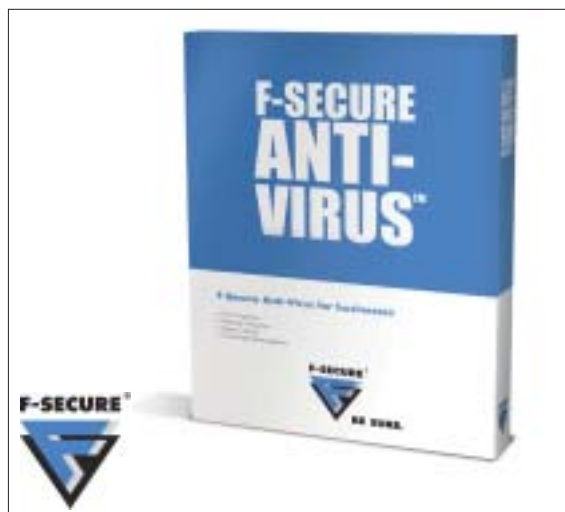
The product installed was F-Secure Internet Security 2004, which includes monitoring of internet traffic and an intrusion detection system as well as the anti-virus functions.

The attractive GUI is clearly laid out, with five buttons labeled Home, Virus Protection, Internet Shield, Automatic Updates, and My Subscription. Home displays a summary of the state of protection of the computer. Updating can be done online and can be scheduled.

Each screen contains a number of buttons that can be used to switch basic settings, plus an Advanced button for more detailed configuration, though this is not necessarily appropriate for the less experienced user.

The Advanced menus include a choice of four general security levels (high/normal/off/custom), the first three of which automatically configure the product to reach the chosen level.

Scanning jobs can be started either from the virus protection screen or from the system menu. A full report is available from the GUI and logs are saved as HTM files, with possible notification of a found virus to a remote user.



News reports are downloaded automatically to the computer to warn of major outbreaks.

The product detected all the virus samples in the test suite, disinfected all appropriate files and also disinfected the pre-infected systems.

THE VERDICT

F-Secure Anti-Virus is a strong, reliable product, ideal for corporate use. It performed well in testing, detecting and disinfecting all samples in the tests, even those hidden in very deeply nested zipped files. Logging and reporting functions are very good.



eScan Internet Security System 2.6 for XP Pro



DEVELOPER'S STATEMENT: The real-time anti-virus and content security product for single users to large networked systems.



Anti-Virus
Level 1

Product: eScan Internet Security System 2.6 for Windows XP Pro
Manufacturer: MicroWorld Technologies Inc.
Contact details: www.mwiti.net/antivirus/
Full White Paper: www.westcoastlabs.org

The installation process for eScan was particularly easy. Once installed, there is a plethora of options. Target files are scanned by default using automatic type recognition, or can be user defined.

eScan detected all files in the functionality tests. In the compression test, eScan detected 12 viruses. Two other files were described as infected with 'Password-protected-EXE'. The product did not report anything on the other four files.

THE VERDICT

eScan detected all samples in our standard tests, and found all samples in the unencrypted deeply nested zipped files. Has many features which are useful in a corporate network.



Panda Platinum Internet Security for Windows XP Pro

DEVELOPER'S STATEMENT: A complete security solution for businesses and professionals. Protects against viruses, hackers, spam, spyware and other Internet-borne threats.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: Panda Platinum Internet Security for Windows XP Pro

Manufacturer: Panda Software

Contact details: www.pandasoftware.com

Full White Paper: www.westcoastlabs.org

The product can be installed either as a standalone version (used here) or in a corporate setup. Installation of Panda Platinum proved to be simple. It is updated online, though updates can also be downloaded manually or obtained by post.

New updates appear daily (more often during outbreaks) and can be automatically installed. In a corporate environment updates can be distributed centrally and out-of-date definitions are reported to the user.

Scanning and hospital

The GUI is clear and well laid out. Tabs at the top lead the user to the update process, the report (all entries for the session appear on the one log), virus information and general options. A menu at the side offers the home page, scanning, permanent protection, hospital and services.

The full scan page is used for launching any on-demand scanning, not just a complete scan of the computer. Permanent protection is for the real-time scanner and the firewall, which come with the product and are both automatically enabled.

Hospital is the quarantine area in which files which have been detected as having viruses are held, while services features general services such as support contacts and links to any other Panda products installed. This area also includes a suggestion box which enables users to send suggestions to the company for improvements to the product.

Panda Platinum Internet Security can scan drives, folders or archived files and also scans incoming and outgoing emails by default. Scans can be scheduled for certain times or launched immediately, while corporate users can be prevented from disabling the real-time scanner. At shutdown the floppy disk drive is checked to deter booting off an infected disk.

Logs, either in their entirety or in part, can be printed off or saved to a file of the user's chosen



format. They can be sorted and the user can choose what will appear in the log. User notifications can be disabled and a remote user notified of any detection.

Virus information is provided on the user's hard drive and suspicious samples can be submitted to the company via email.

Finding the problems

Panda Platinum Internet Security also includes a fully-integrated firewall to deter hackers and protect information, though this was not examined in these tests.

It detected and disinfected all the appropriate files in the main functionality tests. It also cleaned the pre-infected systems.

For the compressed file tests, Panda Platinum detected problems with 12 of the 18 compressed files. No warning that the other six files were encrypted was given. The product detected all the Trojans in the West Coast Labs collection without any problem.

THE VERDICT

Panda Platinum is a good, solid, dependable product that performed very well in testing. It detected and disinfected files and systems, and correctly identified the nested zipped samples, though no warning was given over the encrypted files. The product comes with a range of useful features.



BitDefender 8.0 for Windows XP Pro

DEVELOPER'S STATEMENT: Integrates anti-virus, firewall and anti-spam into one comprehensive security package, tailored to meet the needs of home internet users worldwide.



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: BitDefender 8.0 for Windows XP Pro
Manufacturer: Softwin
Contact details: www.bitdefender.com
Full White Paper: www.westcoastlabs.org

The installation of the recently released version 8 passed off quietly and the product was updated online. Updates can also be downloaded manually. New updates appear daily but more frequent updates are available during emergencies, and automatic updates can be scheduled, or the computer can be set to look for new updates at regular intervals. Out-of-date definitions are reported to the user.

Settings and logs

A striking feature of BitDefender's GUI is that the color scheme can be varied. Mostly grey and white, it comes with a top bar in a cheerful red, which can if so desired be changed to ochre or to a dark grey. Five icons run down the left hand side: general, anti-virus, antispam, firewall and update (for updating the product as a whole). Each icon opens a number of tabbed pages, with basic relevant help information displayed and a path to more if needed.

The general tab contains license information, an overall status summary, and settings relating to the product as a whole. The latter includes the ability to protect settings by making them password-protected, which is not done by default, but is potentially very useful if a family or a number of users share a computer. The anti-virus tab includes Shield (the real time scanner) and Scan (for on-demand scanning), with scheduling, quarantine and reports.

The Scan window shows the local drives, any or all of which can be selected for scanning. Folders and other items can then be added to the range available for scanning.

Default settings include scanning of incoming email and Registry control. The default setting on both real-time and on-demand scanning is to disinfect the infected file, but other options available are Report only, Prompt the user, Delete, Rename, and either Copy to or Move to quarantine.

Two different logs are maintained in files, the



size of which can be limited. By default the latest log overwrites its predecessor, but this can be changed so that it is appended to the previous log. Logs can also be printed off.

There is a virus encyclopedia online and samples can be sent to Softwin online.

Dealing with the problems

In the first two functionality tests BitDefender detected and disinfected all the appropriate files. All pre-infected systems were disinfected without difficulty.

For the compressed files, BitDefender's default setting detected viruses in 12 and the report made no comment on the other six. When the default was changed to list all files scanned, then the six files were marked as being password protected.

BitDefender detected all the Trojans in the West Coast Labs collection without any trouble.

The product's firewall and anti-spam features were not examined as part of this report.

THE VERDICT

BitDefender Professional has been developed squarely for the home user, with options sensibly selected to provide good protection for home use. The product performs well on the default settings and dealt effectively with pre-infected systems.



Symantec AntiVirus Corporate Edition 9.0 for XP Pro

DEVELOPER'S STATEMENT: Combines industry-leading virus protection for enterprise workstations and network servers with centralized management and administration capabilities.



Anti-Virus Level 1



Anti-Virus Level 2



Trojan

| | |
|--------------------------|------------------------------------------------------------------|
| Product: | Symantec AntiVirus Corporate Edition 9.0 for XP Pro |
| Manufacturer: | Symantec Corporation |
| Contact details: | www.symantec.com |
| Full White Paper: | www.westcoastlabs.org |

Symantec AntiVirus Corporate Edition (SAVC) was installed as a standalone product. It installed without any problems and was easily updated. Updates can be downloaded and applied manually or automatically. These are released at least daily, and the computer can be set to automatically download the latest update at start up or at other times. Out-of-date definitions are reported to the user. In a corporate set-up it is possible to distribute updates.

One might expect the GUI to feature the familiar Symantec yellow, but while the real-time icon is a yellow shield, the GUI is in blue, grey and white, a neat and businesslike effect.

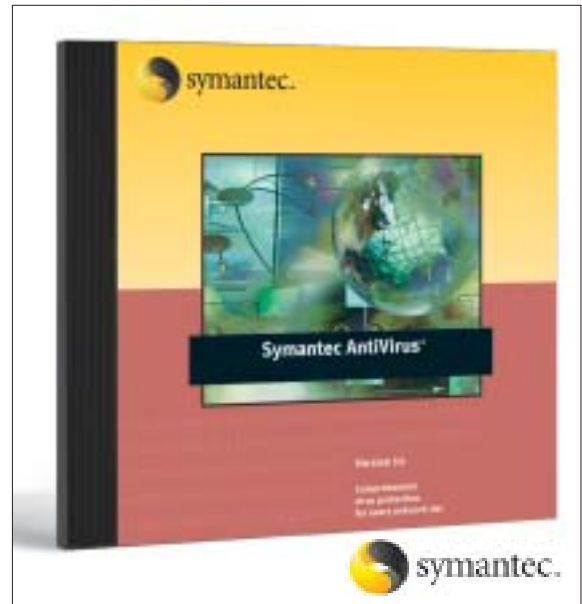
Scanning and reporting

A tree of tasks runs down the left hand side, each branch opening a new screen on the right hand side of the GUI. This enables the user to run and configure scans and resident protection, view logs (here labeled Histories) and perform other work. The same screens can be reached from a series of seven buttons across the top.

Two scan tasks are already created, one scanning hard disks and one scanning removable media. The screens also offer the opportunity to create new tasks, which can then be scheduled for running at start up or at other times, and may be centrally controlled in a corporate setup.

Options available to the user are identical in the main and the real-time scanners: clean (the default), delete, log only, or quarantine. On finding an infection the report names the threat and reports its name as a link to the relevant entry in the online virus encyclopedia.

In addition to the normal real-time scanner, modules exist for scanning internet traffic and incoming email for viruses. Each is on by default, and the email modules (separate modules for Microsoft Outlook and Lotus Notes) are designed to scan both incoming and outgoing traffic heuristically, to prevent spreading of



worms.

Logs cannot be printed immediately but can be saved to a file and then printed off. User notifications can be disabled or they can be routed to a remote user. Virus samples can be submitted to the company online.

Working on clean-up

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files. It also disinfected all three pre-infected systems.

For the tests with compressed files, in SAVC the user can specify how many levels of archives will be scanned. Using the default level of 3, eight viruses were detected. Setting the maximum level of 10, ten viruses of the 12 were detected (the other two were too deeply archived to be found). No comment was made on the six encrypted files.

SAVC detected all the Trojans in the West Coast Labs collection without problems.

THE VERDICT

Performed very well on the detection and disinfection tests. There is an inbuilt limit on how deeply nested zipped files can be scanned and no comment was made on the encrypted files. This product should be considered by anyone looking for a comprehensive AV solution for their network.



Sophos Anti-Virus 3.86 for Windows 2000 Professional

DEVELOPER'S STATEMENT: Sophos Anti-Virus offers total network protection from gateway to desktop, including remote laptops, from the latest viruses, Trojans, worms and spyware.



Anti-Virus
Level 1



Anti-Virus
Level 2

Product: Sophos Anti-Virus 3.86 for Windows 2000 Professional
Manufacturer: Sophos
Contact details: www.sophos.com/products
Full White Paper: www.westcoastlabs.org

Sophos Anti-Virus uses a combination of virus scanning and check summing for on-access protection. Installation was easy and the GUI is functional and uncomplicated. Scans may be 'Quick' or 'Full', with a list of file extensions (which the user can modify) to be scanned. Archives and mailboxes can also be scanned, though not by default.

Scanning information is displayed at the bottom of the GUI screen, though it does not display in its default size; the user must expand the GUI to see the results. A large progress bar shows the relative completion of the job. Logs are automatically written to the hard disk.

The real-time scanner scans incoming mail by default. At shutdown, the product checks that there is nothing in the floppy disk drive, to assist in avoiding boot sector viruses. Another useful facility is that in a corporate environment, it is possible for the administrator to freeze the settings by requiring that a password be entered before any setting can be changed.

In functionality testing the product detected all the virus samples in the test suite and



disinfected all appropriate files. In Test 3 it failed to modify or remove one file pre-infected with W32/Korgo.A. Of the 18 compressed files, 12 were detected with infections, but the six encrypted files were not reported as such.

THE VERDICT

Sophos Anti-Virus performed very well in the standard tests and identified samples in zipped files, even those that were very deeply nested. Management tools allow for centralized installation, configuration and monitoring making it a good choice for the corporate environment.



Tegam ViGuard 10.23



DEVELOPER'S STATEMENT: Enterprise desktop protection, independent of known virus signatures. Central administration and policy for small-to-medium enterprises and individuals.



Anti-Virus
Level 1

Product: ViGuard 10.23
Manufacturer: Tegam
Contact details: www.viguard.com
Full White Paper: www.westcoastlabs.org

ViGuard is a standalone product that does not rely on scanning as such but upon a mixture of detecting viral ability when a file is run, identifying suspicious macros and protecting system files and processes against alteration. Upon installation it scans the system

and identifies system vulnerabilities.

Drives or folders can be verified. This process involves scanning the files to identify their characteristics and code, so that alterations can be detected and, if necessary, reversed.

In the tests all infected files were intercepted upon running.

THE VERDICT

ViGuard's unusual virus detection does prove to be effective. It is efficient and thorough against today's AV threats and should continue to be so in the future.



OfficeScan Corporate Edition 7.1 for Windows XP Pro

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



Anti-Virus
Level 1



Anti-Virus
Level 2



Trojan

Product: OfficeScan Corporate Edition 7.1 for Windows XP Pro

Manufacturer: Trend Micro

Contact details: www.trendmicro.com/en/products

Full White Paper: www.westcoastlabs.org

OfficeScan Corporate edition has to be installed via a Management Console on a server and then the client installation deployed to machines connecting to the server. Using the console the administrator can choose the default settings for the client installations which will be deployed on to the users' machines, and can also choose whether to allow the users to change these settings – they will not be able to do so without specific permission.

Updates can be downloaded on to the server and then deployed to the clients, downloaded directly to the client, or the files can be downloaded manually and applied to the machine. Updates can be scheduled, and new pattern files are produced each day, more often during outbreaks. The user is informed if virus definitions are out-of-date.

Settings and scanning

The client's GUI is neat and workmanlike, with three buttons at the top: File, Options and Help. Options is grayed out if the user is prevented from altering settings as it is for configuration. This could be seen as a minor drawback in that the user can't see exactly what settings are in use. Five tabs labeled Scan, Scan Results, Mail Scan, Log Report and Toolbox each open a new window in the GUI.

The user can launch scans and the administrator can also schedule scans centrally. During the scan another box opens, showing the name of the file being processed and a progress bar. Options on detection of a virus are Clean (the default), Delete, Pass, Quarantine and Rename. The real-time monitor can Clean (the default), Delete, Deny Access To or Quarantine a virus. When the results are shown, clicking on the virus name will open the relevant entry in the online virus encyclopedia.

In the Mail Scan window, the user can set up scans of POP3 and Outlook mail, although this



is not the default. In the Log Report window, all logs for a certain period can be seen in a concatenated form; the default setting is that logs are deleted after fifteen days. The Toolbox window enables installation of Wireless Protection Manager and Check Point SecureClient.

Detecting and disinfecting

In functionality testing the product detected all the virus samples in the test suite and disinfected all appropriate files. It also disinfected all pre-infected systems.

For compressed files, the default level of compressed layers that will be scanned is two. Using this setting, eight out of the 18 files in the test were identified as having viruses. After changing to the maximum setting of 20, 12 files were identified as being infected. No files were mentioned as encrypted.

The product detected all the Trojans in the West Coast Labs collection.

THE VERDICT

OfficeScan is clearly aimed at the larger company, and is designed to assist the central administrator in maintaining firm control. Very dependable detection and comparatively fast scanning back up the product, which any large corporate organization will want to consider in its AV defenses.



Contact information

West Coast Labs,
Haymarket Media Inc.,
Floor 3, 114, West 26th Street,
New York, NY 10001, USA.
Tel: +1 646 638 6000



West Coast Labs,
West Coast Publishing,
William Knox House,
Britannic Way, Llandarcy,
Swansea, SA10 6EL, UK.
Tel: +44 (0) 1792 324000

For more information, contact Chris Thomas by email cthomas@westcoast.com • www.westcoastlabs.org