

TECHNOLOGY REPORT - OCTOBER 2005

AntiVirus & Trojan Solutions

An Independent Technology Report produced by



www.westcoastlabs.org

Product Testing, Evaluation and Certification Services



West Coast Labs provides a superior quality testing and certification service for infosecurity technology developers and has established independent industry-accepted standards on product effectiveness and performance for the benefit of corporate end-users and decision-makers alike.

Through its global reach, West Coast Labs brings technology developers and corporate end-users together, creating a meaningful link between what the market needs and what technology developers are offering.

West Coast Labs Services

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

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



www.westcoastlabs.org

Comment

Server-based solutions to protect your network from viruses and malware



Jon Stearn
CTO, West Coast Labs

Welcome to this, the fourth Technology Report to be published by West Coast Labs in 2005. In this report we look at a range of server-based antivirus solutions, which aim to provide an administrator with defenses against malware at different points on the network. All the products

featured have achieved certification under the Checkmark scheme, and are thus regularly tested to confirm their ability to detect all viruses in the wild at the time of testing.

The range of solutions is impressive, and can be divided into three main categories. There are antivirus solutions which are intended to protect files stored on a file server, antivirus mail gateways and fully fledged gateway solutions. Many of the products under review form part of a complete network antivirus suite.

Multi-system protection

Those who are looking for protection for Unix or Linux based systems are not neglected either. We consider two solutions which provide antivirus capability on a Linux file server, and include the capacity to scan for Linux, Macintosh and Windows viruses. Although there are far more Windows-based viruses, they do exist in the Mac and Linux world too.

Of the mail gateways under review, some are intended to integrate with a particular mail system, like Microsoft Exchange Server. Others provide generic support for any SMTP traffic.

Informing your decisions

At the gateway level, we consider some products which aim to screen infected files at the point of entry to the network using a variety of common protocols.

As always, our aim is to provide objective information on the results of our testing, and information on the features and functionality of each product, to enable you to make an informed purchasing decision and choose the product that is right for you. Full information on the products featured, together with a detailed buyers' guide can be found online at www.westcoastlabs.org.

Introduction

Creating the environment for a small or medium business in our controlled testing

The overall objective of this antivirus and Trojan Technology Report for server, appliance and gateway solutions is to evaluate each product in a controlled environment. Throughout the test period, each product was configured as recommended to update online. The testing environment represented that of a small to medium-sized business or branch office.

Products were tested in accordance with the functionality criteria of the Checkmark certification system for Antivirus Level 1 and, where Checkmark Certification registration permitted, for Antivirus level 2 and Trojan.

Each test report is supplemented by a features and functionality Buyers Guide, and information from the product developer concerning the type of business or organization the product is developed for, plus the direct technical and business benefits of the product. Each white paper looks at a product's management, administration and functionality.

1. Management/Administration.

The testing reports on the following functions:

- Installation
- Product update process
- Logging and reporting function

2. Functionality

Products are tested in accordance with Checkmark AV level 1 and Trojan test (where registered) to determine the ability to detect viruses and Trojans. For those products registered for Checkmark AV Level 2, the testing will report on the following virus disinfection capabilities:

- Products will be tested to determine their ability to disinfect files infected with viruses.

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, Richard Thomas, Mike McMenamin and Chris Elias.



Introduction continued...

- Products will be installed onto systems previously infected with specific viruses.
- The ability of the product to counter and remove the infection will be assessed.

What is a virus?

A virus is a program or piece of code attached to a file or diskette's boot sector and is loaded onto a computer without the user's knowledge. Viruses are manmade (though they can be corrupted in use to form new variants of the virus) and replicate themselves by attaching themselves to files or disks, often soaking up memory or hard disk space and bringing networks to a halt. Most recent viruses are internet-borne and are capable of transmitting themselves across and bypassing security systems. Minor variants of the same virus are classed as families of viruses.

What is a Trojan?

Trojan horses or Trojans are destructive programs that pretend to be benign applications. Unlike viruses or worms, Trojan horses do not replicate themselves, but they can be damaging to networks by delivering other types of malware

Find the full results online

The analysis and full test results for each solution, which include both functionality and performance data, are online at www.westcoastlabs.org along with white papers, buyer's guides and other product information.



West Coast Labs Photographs Copyright Girts Gailans www.gailans.com
Art editor: Sarah Lloyd, Sub-editor: Alison Walley

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

Check for the Checkmark



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

eTrust Antivirus for Windows 2003 server

DEVELOPER'S STATEMENT: eTrust Antivirus is a comprehensive anti-viral defense solution with scalable and sophisticated management capabilities to suit any enterprise, whether large and complex or small to mid-sized.



Product: eTrust Antivirus 7.1 for Windows 2003 server
Manufacturer: Computer Associates, Inc.
Contact details: www3.ca.com/solutions/

There are two scanning engines in eTrust Antivirus: the longstanding CAI product, Inoculate, and another well-established product, Vet. This report's tests were run against the Inoculate engine, although either product can be used.

The product can be used as an administration server controlling other machines, and in a corporate setup it is possible to distribute updates. We installed and tested the product in standalone mode and installation was uncomplicated. We updated the product online, although it can also be updated manually using downloaded updates. Updates are either full or incremental and it is important to note that they are for the individual engines only, so that whichever one is in use, the specific update must be downloaded.

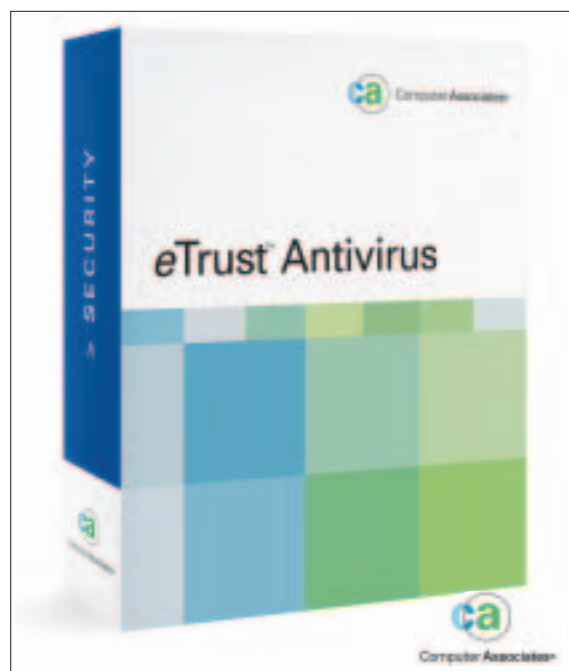
New updates appear daily, more often during virus outbreaks, and automatic updates can be scheduled. The user is warned if the product has not been updated. Two methods of scanning are offered, Secure and Thorough. We used the default setting, Secure.

A practical and uncluttered interface features four buttons across the top: File, Scanner, View and Help. The user can page between two screens with the View button, the first of which displays the possible scanning targets while the second shows the various logs available to the user. When the second screen is displayed, a button labeled Log is substituted for the Scanner button.

The File button offers printing facilities and the Help button not only shows help information but also has a link to online virus encyclopedia facilities.

The Scanner button takes the user to the center of activity. Here the user can choose what should be scanned from the various targets shown (drives, folders, etc.). Directories and subdirectories can be displayed and selected by clicking the folders in the chosen drive. Any combination of files and directories can be selected for scanning. Details of any infected files found in the current or last scan are displayed at the bottom of the screen.

Both local and real-time scanners can Cure (disinfect), which is the default, Delete, Rename, Move or merely Report on an infected file. If the file cannot be disinfecting (Unrepairable) the options available are



Move, Rename or No Action (the default). The two scanners can be configured separately.

The Scanner screen also allows access 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.

On the log screen the various different logs are divided according to the type of scanning engine that produced them, each section showing a separate list of the reports available for that particular engine. Logs can be printed or saved in a file, either partially or wholly.

Using the definitions of 31 August, eTrust detected all the viruses in the June Wildlist and disinfected the appropriate files. It also detected all the Trojans in the West Coast Labs collection without problems.

The product's ability to detect spyware or adware was not examined as part of this report. Equally, its abilities to deploy to and control other machines were not investigated.

THE VERDICT

eTrust AntiVirus provides comprehensive protection against viruses and Trojan threats, through the use of two separately configurable scanning engines. The GUI is easy to use and well laid out and provides all the management tools needed in a network setting.



*The eTrust
AntiVirus from CA
is Checkmark
certified to
AntiVirus Level 1,
2 and Trojan.
www.check-mark.com*



NOD32 AntiVirus System 2.50 for Windows 2003 Server

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



Product: NOD32 AntiVirus System 2.50 for Windows 2003 Server
Manufacturer: Eset Software
Contact details: www.nod32.com

NOD 32 installed without any difficulty, although one rather strange setting was noted: installing the typical configuration with no alterations means that the resident protection is not automatically started. To be fair, a screen asks the user to remove any other resident protection and then strongly recommends that the appropriate box is checked, but anyone clicking through the screens without paying full attention could find that the end result is a system with no resident protection running. The product updated without problems.

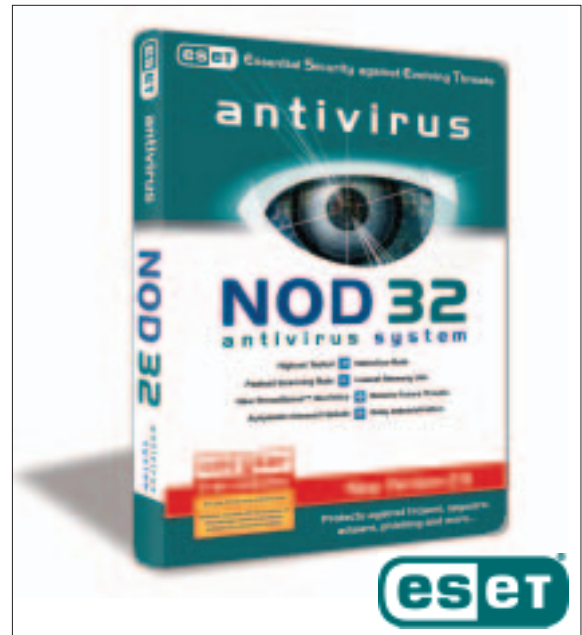
The product when installed is in two almost disconnected parts: NOD32 and NOD32 Control Center. From the menu bar both NOD32 and NOD32 Control Center can be started.

An icon also leads to the Control Center where settings for the four monitors can be controlled. NOD32 has a separate set of screens from which manual scans can be run. Both sets of screens are functional and unfussy.

The Control Center lists the four monitors (files, documents, email and Internet protection), each of which can be configured separately. These settings are independent of those set in NOD32, so that for instance each monitor and the manual scan can all use separate lists of extensions. Each of the four monitors can be enabled or disabled, the icons turning red if the relevant monitor is disabled, so that the user is aware of the monitor's inactivity. Special settings are used for scanning newly created or modified files. (A link to the other part of the product enables manual scans to be targeted and run, but from here the settings cannot be altered – that must be done in the manual scanner screens.)

In NOD32 all the usual settings for manual scans can be found and configured. By default scans are run against a list of extensions which the user can amend, but scans can be changed to scan all files, including those with no extension. Different actions can be set for malware found in files, boot sectors and memory. Settings can be saved in profiles that can then be allocated to various types of scanning (e.g. scanning of folders or of removable media).

Archives, self-extracting archives and email files can



be scanned but are not done so by default in manual scanning, although the Control Center monitors do scan them by default when created or modified. NOD32's default settings include the use of virus signatures, heuristics and adware/spyware but not advanced heuristics and potentially dangerous applications such as spyware, which are also available within the product.

Logging can be enabled or disabled, with the entries written to a file of your choice. Entries for this file can either be appended or overwritten, and the maximum size of the log file can also be set.

Using the definitions of 19 August, NOD32 detected all the viruses in the June Wildlist without problems and disinfected the appropriate files. It also detected all the Trojans in the West Coast Labs collection without problems.

The product's ability to detect spyware or adware was not examined as part of this report. Equally, its abilities to deploy to and control other machines were not investigated.

THE VERDICT

It may take a little time to become familiar with the arrangement of NOD 32's settings but the accustomed user will be able to achieve even better results with this reliable and efficient product. Overlook it at your own risk.



The NOD32 from Eset is Checkmark certified to AntiVirus Level 1, 2 and Trojan.
www.check-mark.com

Kaspersky Anti-Virus 5.0 for Windows File Servers

DEVELOPER'S STATEMENT: Two-tier data protection for servers against malicious code: an antivirus monitor which scans all accessed, newly created and modified files in real time, and an antivirus scanner which scans data storage locations.



Product: Kaspersky Anti-Virus 5.0 for Windows File Servers
Company: Kaspersky
Contact details: www.kaspersky.com/products

Kaspersky Anti-Virus for Windows File Servers (KAV) comes in the form of a command line scanner, although it is also possible to add a freeware administration utility, Kaspersky Administration Kit, which can be used to deploy and administer Kaspersky Anti-Virus in a corporate environment and across networks. We tested it as a command line scanner.

The command line executes a program KAVSHELL which has a number of options, most having their own switches.

SCAN can be used to scan selected items (files, directories, memory, network drives, removable media), while FULLSCAN scans the entire drive. In both of these cases the user can choose to scan by file type or by file extension, as well as all files – archives and compressed files are included. Infected files can be deleted or disinfected, but if neither switch is chosen the files are left unaltered.

Each scan can be directed to save output in a text file of the user's choice, and the text inserted into the file can be either the entire output or merely what Kaspersky considers to be the more important lines. If the name of a file already in existence is chosen, the contents are not overwritten or added to, but a new file is created with a modified name.

Updates can be done online, using the UPDATE switch, but it is not possible to schedule updates; if an update proves to be unsatisfactory in some way the ROLLBACK command will return the databases to their previous state.

RTP controls the perhaps rather slow but certainly effective real-time scanner. This can be stopped or started (by users with administrator status) and again output can be saved in a text file.

TASK will control specific tasks; some of these have been set by Kaspersky, others can be set by the user. They can be started or stopped but cannot be scheduled.

START and STOP can be used to start or stop the whole product – but only a user with administrator status can do this.

A tool assisting performance is iChecker, which stores checksums of uninfected scanned files in a database,



and then confines scanning only to those files added or altered since the last scan.

Although the detection rate for Kaspersky Anti-Virus for Windows File Servers was only tested using the command line, there is also a free administration utility available from Kaspersky's website, although this is a rather hefty 37.59Mb download. This gives the option of adding an administration server or administration console. The administration server requires either SQL Server installed, or the MSDE2kSP3 installer that is also available from Kaspersky's site (an extra 31Mb download).

The GUI makes the implementation of functionality much easier than the command line in that it becomes possible to easily schedule scans and set up alerts with only a couple of clicks. If the full administration server is installed, then there is the possibility of deploying to other machines within a domain with a simple wizard format that provides a variety of options, all well labeled and easy to follow.

Using the definitions of 25 August, KAV detected all the viruses in the June Wildlist without any trouble and disinfected the infected files and disks. It detected all the Trojans in the West Coast Labs collection.

THE VERDICT

Kaspersky's command line scanner contains all the detection ability of its other products, and the additional GUI simplifies implementation of its functionality. Useful features such as iChecker and strong detection mean that Kaspersky Anti-Virus cannot be dismissed from consideration.



The Kaspersky Anti-Virus for Windows File Servers is Checkmark certified to AntiVirus Level 1, 2 and Trojan.
www.check-mark.com



McAfee VirusScan Enterprise 8.0i for Windows 2000

DEVELOPER'S STATEMENT: McAfee VirusScan Enterprise 8.0i provides advance, proactive protection from malware for PCs and servers. It contains functionality for antivirus, host-intrusion prevention (HIPS) and firewalls, for protection from known and unknown attacks.



Product:	McAfee VirusScan Enterprise 8.0i for Windows 2000 Professional
Manufacturer:	McAfee, Inc. (Network Associates Technology, Inc.)
Contact details:	www.mcafeesecurity.com

VirusScan Enterprise installed without any problems and was easily updated. Updates can either be downloaded manually or applied automatically. These updates can be obtained for engine and database separately, or they can be combined into Superdat files. These are released daily, with more frequent updates available during emergencies, and the computer can be set to automatically download the latest update at start up. In a corporate setup it is possible to download one update and distribute it across the network.

Although the design of the interface for VirusScan Enterprise has remained unchanged for some time, the upgrade from version 7 to version 8 considerably altered the tasks available to the program. New tasks include buffer overflow detection, unwanted programs policy and access protection (port blocking rules).

Beyond these three tasks are all the usual ones that the user would expect to be available, such as scanning the hard disk, scanning email (incoming email is scanned by default) and updating. The interface 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.

Actions available to the scanner are: Clean (the default), Continue the scan, Delete, Move or Prompt, while the real-time scanner can deny access, clean (the default), delete or move. 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.

The access protection option enables the user to block traffic through ports as he or she chooses. This means it is possible to lock down ports, so that viruses coded to use a particular port will either not infect a system or be ineffective when that port is unavailable. It thus becomes possible to disable those viruses trying to infect the computer across the Internet or another network, or trying to send or download files across a network. Buffer overflow detection prevents the execution of arbitrary code on the machine, another favoured tool of virus writers.



The unwanted programs policy enables the user to expand detection beyond viruses to include categories such as spyware and adware. These categories are turned off by default and must be chosen individually. Users should note that when adding a new task, a box enables the detection of unwanted programs. Turning this on uses the settings defined in the unwanted programs policy; however, if none of the categories there have been selected, then turning on detection of unwanted programs in a task has no effect. In these tests, detection of items offered as unwanted programs (e.g. adware) was not tested.

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

It is possible to configure the program by remote access, and in addition local users can be prevented from changing settings (e.g. from disabling the real-time scanner) unless a password is entered.

Using the Superdat file 4564, created on 22 August, VirusScan detected all files in the June Wildlist and disinfected all the infected items without problems. It detected all the Trojans in the West Coast Labs collection.

THE VERDICT

VirusScan enterprise provides an administrator with all the tools required to implement a comprehensive, manageable antivirus policy on the network. The product provides excellent detection of viruses and Trojans, and infected files can be disinfected quickly and capably.



The VirusScan Enterprise 8.0i from McAfee is Checkmark certified to AntiVirus Level 1, 2 and Trojan.
www.check-mark.com

Panda FileSecure Antivirus

DEVELOPER'S STATEMENT: Panda FileSecure with TruPrevent Technologies is the perfect solution for protecting Windows and NetWare file servers with a minimal use of system resources against known and unknown viruses and other threats.



Product:	Panda FileSecure
Company:	Panda Software International
Contact details:	www.pandasoftware.com/products

Panda FileSecure is a component of Panda EnterpriSecure with TruPrevent Technologies, which in this case was installed and administered using Panda AdminSecure, another component of the EnterpriSecure suite.

We installed Panda AdminSecure to a Windows 2003 server, where it created an administration console supervising all available devices. We then deployed it to a Windows 2003 server on which it installed Panda FileSecure; had we deployed it onto other platforms, it would have installed other modules of EnterpriSecure.

The networking ability of this product allows for distribution over a wide network to a variety of other systems. The ability to schedule scans at different times for different groups or different individual clients is useful to ensure that the administrator with responsibility for keeping the clients secure is not overwhelmed at any one time.

Distribution of the Communications Agent is simple and straightforward. A wizard allows the administrator to install it remotely, to generate a script to install it on the next user login, or to build a package for some other means of distribution. It is a very simple procedure to follow, and takes a lot of the work of distribution away from the administrator.

Once installed, real-time protection runs on the client machine but all scans are initiated and controlled from the AdminSecure machine. The user of the client machine sees the real-time monitor's Panda-face icon but can do nothing with it.

The AdminSecure console can be opened on the server machine without any password. It contains a list on the left comprising Windows workstations and various server types. Categories not in use can be hidden to reduce the details displayed and make it easier to concentrate on relevant information. At the bottom of the list are two buttons, Administration and Reports. Reports of a number of different types can be generated and Administration returns the user to the original screen.

Clicking on any server type brings up a list of the members of that category currently known to AdminSecure. For each of the server categories a screen on the right shows six tabs: Self-Diagnosis,



Modules, Jobs, Settings, Scan and Events. Overall, the interface is easy to navigate and well organized.

Self-diagnosis provides statistics for the members of the category, such as how many have antivirus installed, how many have outdated definitions and how many are disabled. It also provides links by which any problem in these categories can be corrected. Modules lists the members of the category, and right clicking on each member means that it can have the antivirus installed, removed or updated; scans can be added and settings edited.

Settings also enables these to be edited. The defaults are use of an editable extension list for scanning (though all files can be selected) and that malware will be detected. Possible actions on detection include delete, disinfect and rename. Warnings can be sent and heuristics can be used. Events provides a log of the problems found on that machine.

AdminSecure's online services include virus information, technical support and the latest documentation.

Using the definitions of 29 August, Panda FileSecure detected and disinfected all the viruses in the June Wildlist without any trouble. It also detected all the Trojans in the West Coast Labs collection.

THE VERDICT

FileSecure from Panda is a component of the EnterpriSecure suite which offers complete antivirus protection across a heterogeneous network infrastructure. It provides excellent detection of virus and Trojans, and is recommended for any administrator with a complex network to administer.



The Panda Filesecure is Checkmark certified to AntiVirus Level 1, 2 and Trojan.
www.check-mark.com

Symantec AntiVirus Corporate Edition

DEVELOPER'S STATEMENT: Symantec AntiVirus Corporate Edition combines industry-leading virus protection for enterprise workstations and network servers with centralized management and administration capabilities



Product:	Symantec AntiVirus Corporate Edition
Manufacturer:	Symantec
Contact details:	www.symantec.com

Symantec AntiVirus Corporate Edition (SAVCE) has three installation options: local, client or server. In this case SAVCE was installed as a standalone product.

If the server installation is deployed then it is possible to install the System Center as a further option. This uses the Microsoft Management Console as the interface. It is possible to schedule scans on remote machines or the server itself, with the option to send quarantined files to a special quarantine server.

Distribution of the client application is easily handled and the Help file provides detailed instructions. Once the client applications have been installed, it is then possible to remotely manage all the clients from the central console. There is the ability to flash up a message on the remote client machine detailing any suspicious files found and what actions have been taken.

SAVCE installed without any problems and was easily updated. Updates can be downloaded manually (intelligent updater – weekly) or automatically (live update – at least daily). More frequent updates are available during outbreaks, and the latest update can be automatically downloaded at start up or at other times. Out-of-date definitions are reported to the user.

A tree of tasks runs down the left-hand side of the main screen, each branch opening a new screen on the right. Here the user can run and configure scans and resident protection, view logs (here labeled histories) and perform other required work.

Four scan tasks are available: Floppy disk (removable media); Quick Scan (memory and the most commonly infected areas of the hard drive); Full Scan; and Custom Scan. The user can also create new tasks that can then be scheduled to run at start up or at other times, and can be centrally controlled in a corporate set-up.

The main and real-time scanners have identical options: Clean, Delete, Log only or Quarantine. Different settings can be allocated to macro viruses and non-macro viruses, while security risks can be given a generic response that can then be overruled for specific types of malware such as adware or spyware. When an infection is found the report names the threat and provides a link to the relevant entry in the online virus



encyclopedia.

In addition to the real-time scanner, modules exist for scanning Internet traffic and incoming email for viruses, with separate modules for Microsoft Outlook and Lotus Notes. Each is on by default, and the email modules scan both incoming and outgoing traffic heuristically, to prevent spreading of worms. An additional real-time protection, Tamper Protection, has been added in this version to protect the Symantec tools from being infected or closed by viruses or other malware.

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

Dealing with this product is very easy and the integration with Symantec Client Firewall, providing central management, is an additional benefit that should not be overlooked.

Using the definitions created on October 23 SAVCE detected all files in the June Wildlist without any difficulty and disinfected the infected files and disks. It also detected all the Trojans in the West Coast Labs collection using the definitions of August 23.

THE VERDICT

Symantec AntiVirus Corporate Edition's recent upgrade has maintained its usual high standards, and the introduction of the important tamper protection shows Symantec's commitment to improving the product. Ease of use and copious facilities make this a product that must be considered.



Symantec AntiVirus Corporate Edition is Checkmark certified to AntiVirus Level 1, 2 and Trojan.
www.check-mark.com

Sophos Anti-Virus 4.5.3 for Windows NT Server

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.



Product: Sophos Anti-Virus 4.5.3 for Windows NT Server
Manufacturer: Sophos
Contact details: www.sophos.com/products

Sophos Anti-Virus was tested as a standalone product rather than in a corporate set-up. It installed easily.

Updates are released daily and can be downloaded online. A new version of the product is released each month, which normally incorporates all signature updates released since the previous version.

The GUI is crisp and straightforward. Buttons provide links to an Internet virus encyclopedia and configuration screens, while large Go and Stop buttons make it very clear how to run the scans. Immediate, Scheduled and On Access tabs control the relevant tasks, and each may be configured differently.

Configuration offers two different settings for scans: Normal (the default) or Extensive. Users can modify the list of file extensions to be scanned using the Options tab. Incoming email is scanned by default, and users may choose to scan mailboxes and archives.

Drives and folders can be selected or deselected for scanning by clicking. A large progress bar gives a clear indication of how much of the current scan has been completed. Scanning and status information is also displayed at the bottom of the screen.

Logs are automatically written to the hard disk and the

Sophos Antivirus 4.5.3 is Checkmark certified to AntiVirus Level 1 and 2.
www.check-mark.com



user can select the destination directory of his or her choice. At shutdown, a summary of the RealTime Scanner during the session is given.

In the functionality tests, using the 18 August definitions, Sophos Anti-Virus detected all the viruses and disinfected the appropriate files without any problems.

THE VERDICT

Sophos Anti-Virus can be centrally managed and monitored across an enterprise network or run as a standalone. The product provides both real-time and on demand scanning, which can be separately configured. Detection of viruses in either mode is excellent.



Vfind for Linux



DEVELOPER'S STATEMENT: Vfind is a scanning engine that analyzes data streams for malicious patterns. It's a proven scanning engine for securing UNIX and Windows for the enterprise.



Product: Vfind for Linux
Manufacturer: Cybersoft, Inc.
Contact details: www.cybersoft.com

We installed VFind on to a Red Hat 9 box. Some minor problems were encountered as certain files were in directories other than those in which the program expected to find them, but after they had been copied, all went smoothly.

We used the program in command line mode, although a VFind Security Toolkit Admin utility can be

opened as a web interface.

The scanner scans a file's contents to identify its file type before examining it for infections relevant to that type. This avoids an infection being smuggled on to a 'protected' system in a file with a misleading extension.

Using the definitions of 24 August, VFind detected all the viruses in the June Wildlist in on demand scanning without problems.

THE VERDICT

CyberSoft VFind runs under Linux, but antivirus protection extends to Windows, Linux and Macintosh. Ideal for use on a Linux file server in a mixed environment.



Cybersoft Vfind for Linux is Checkmark certified to AntiVirus Level 1.
www.check-mark.com



Norman Virus Control 5.0 Corporate for Lotus Domino

DEVELOPER'S STATEMENT: Norman Virus Control is a collection of antivirus software applications and utilities based on the advanced core technologies of Norman's Scanning Engine that protect your workstations, servers and gateways against malicious software.



Product: Norman Virus Control 5.0 Corporate for Lotus Domino server
Manufacturer: Norman
Contact details: www.norman.com

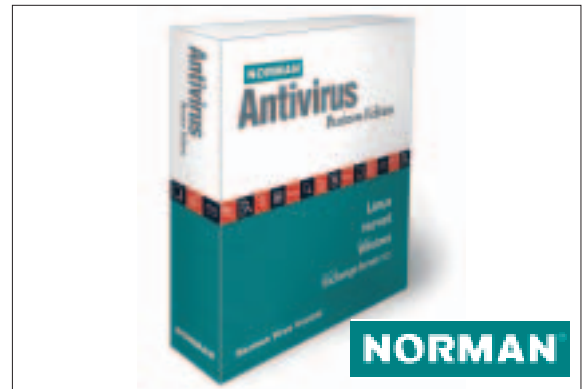
Norman aims its security software in particular at small and medium-sized organizations, where Norman Virus Control (NVC) can be installed as a gateway protection.

The product can be set to be updated online automatically or to search for updates on a LAN or WAN, so that a single Internet update can be used to percolate the latest files throughout a corporation.

Norman Program Manager offers a view of the installed components and message handling and routing services. Norman Virus Control also displays a list of components, but more significantly controls all the configurable settings for the on-demand and on-access scanners. Most importantly these include the Norman Sandbox, which runs all applications in a simulated computer environment, helping to detect unknown threats before detection patterns can be provided.

Other categories that can also be scanned for are security risks and adware. Internet protection automatically covers SMTP, POP3, newsgroups and incoming instant messaging. Certain attachments can also be blocked, including those with double extensions and encrypted attachments. Mass-mailer messages can be stopped, warning messages can be sent to the

Norman Virus Control is Checkmark certified to AntiVirus Level 1, and Level 2.
www.check-mark.com



(apparent) originators and archives can be analyzed or blocked, but none of these is done by default.

The ability to perform on-access scanning during both database access and replications adds to the ability of this software to serve any Domino-based organization well.

Using the definitions of 29 August, NVC detected all the viruses in the June Wildlist without any trouble and disinfected the appropriate files without difficulty.

THE VERDICT

Ease of maintenance and the Norman Sandbox make consideration of Norman Virus Control essential for anyone in its chosen market. Careful attention to its configuration options will reap further dividends, though less experienced administrators can safely use the defaults.



Virusbuster MailShield for SMTP



DEVELOPER'S STATEMENT: A mail system-independent product, which can be easily integrated and flexibly configured to establish a comprehensive line of defense for email traffic against viruses and spam.



Product: VirusBuster MailShield for SMTP
Manufacturer: VirusBuster Ltd.
Contact details: www.virusbuster.hu/en

MailShield is designed to run on a mail server running Linux, OpenBSD, FreeBSD, Sun Solaris or AIX. We tested it under Linux.

It is a command line product with no interface. A command will produce a screen of statistical information, with more detailed information in three logs.

Three depths of virus scanning are fast, strict and full,

with heuristic capabilities assisting detection of unknown viruses.

Other features include a Wormbuster designed to block Internet worms and the ability to delete all macros found in attachments.

Using the definitions of 26 August, MailShield detected all the viruses in the June Wildlist in on demand scanning without any difficulty.

THE VERDICT

VirusBuster MailShield runs under Linux or varieties of Unix. The product can be deployed in a variety of scenarios, and configured to implement a complete email policy.



VirusBuster MailShield for SMTP is Checkmark certified to AntiVirus Level 1.
www.check-mark.com

Trend Micro InterScan Messaging Security Suite 5.5

DEVELOPER'S STATEMENT: Trend Micro InterScan Messaging Security Suite provides antivirus, anti-spam, and content security on an integrated platform for the gateway. Policy-based administration tailors security to meet enterprise requirements.



Product: InterScan Messaging Security Suite 5.5
Manufacturer: Trend Micro
Contact details: www.trendmicro.com

Trend's InterScan Messaging Security Suite (IMSS) is a mail gateway sitting between the outside world and the network's most critical entry point, the email server. It is designed to intercept emails arriving or leaving a site, to investigate them and their attachments and then either to deliver them or to take a designated action.

IMSS is an integrated content security solution operating on a single, server-based platform, blocking a variety of malicious code, although for the purposes of this Technology Report, we only looked at the solution's ability to deal with viruses and Trojans.

Installation of the product was uncomplicated. During this process IMSS offers the ability to install analysis for both SMTP and POP3 - both are installed by default but either can be deselected. This selection is repeated within the configuration so that a service not originally installed can later be selected.

The main interface has a column on the left in a soothing blue, with a large window on the right displaying the settings and modifications available for each area chosen. These are divided into two groups: Configuration and Policy Manager.

Configuration is used for the general settings of the product, containing subjects such as compression, the site of the working directories, notification, encrypted messages, logs, updates and password changing.

Compressed files can be scanned to a depth of 20 compressions, and limits can also be set for the number of files within them and the size of the compressed file, the defaults being 50 and 20 Mb.

Separate logs are maintained for viral infections, other undesirable items found and system messages, and there is also a general log maintenance area. Updates can be scheduled as well as performed immediately, but they are not scheduled by default.

The centralized policy-based functions allow management through individual filters, which are activated and configured as required, depending on the specific business or corporate environment in which deployment occurs.

For this test only the virus filter was used, but other filters available include those for spam, searching for undesirable content such as profanity and pornography,



for hoaxes and chain mail, and the ability to block HTML script.

All of these filters, including the virus filter, are inactive by default and need to be activated by the user if required. Each filter comes with its own group of settings. This screen can appear dauntingly full of options but it is easy to maneuver around it and to find the desired setting.

Users can be grouped in address groups so that all mail going to that group can be handled in the same way. Options available include Delete, Deliver and Quarantine (each of which can include a notification of the infection), and these can be applied to either or both incoming and outgoing mail.

Infected attachments can also be cleaned, although we hit a minor problem here - attachments infected with mass mailing viruses were first cleaned then deleted by a second setting before they could be delivered. Alteration of the second setting enabled the delivery of the disinfected attachment.

Viruses in the June 2005 Wildlist were scanned and were all detected by IMSS. Similarly, it disinfected all the infected files and disks, and detected all the Trojans in the West Labs collection without difficulty.

THE VERDICT

IMSS is a mail gateway that can be deployed to provide complete protection for both inbound and outbound SMTP and POP3 traffic. It provides disinfection of infected mail and attachments, as well as accurate detection of viruses and Trojans.



InterScan
 Messaging
 Security Suite 5.5
 is Checkmark
 certified to
 AntiVirus Level 1,
 2 and Trojan.
www.check-mark.com



Aladdin eSafe Gateway



DEVELOPER'S STATEMENT: eSafe is a gateway-based, integrated content security solution that effectively filters spam, viruses, worms, spyware and file-sharing applications, with fast content scanning.



Product: eSafe Gateway
Manufacturer: Aladdin Knowledge Systems
Contact details: www.aladdin.com/esafe

Aladdin eSafe Gateway is Checkmark certified to AntiVirus Level 1. www.check-mark.com

Aladdin has designed eSafe Gateway to be the sole link between a company and the outside world. The eConsole or Operation Monitor displays a grid showing what has arrived at the Gateway. A pie chart focuses on one particular medium; a graph shows traffic flow from the active protocols.

The Configuration section has a multitude of possible controls. Each protocol (FTP, HTTP, SMTP and POP3)

can be given instructions to block or trust traffic from certain sites and IP addresses.

This area also holds content filters for specific dangers, and controls anti-spam and spyware settings. The administrator can choose how specific types of events will be logged.

eSafe Gateway detected all the viruses in the June Wildlist without difficulty.

THE VERDICT

eSafe Gateway can at first seem a little overwhelming, but an experienced administrator will use its features to provide effective control over external traffic.



NetPilot Plus



DEVELOPER'S STATEMENT: Equinet specializes in the manufacture of multifunctional SmartUTM appliances that provide secure Internet access for small and medium sized enterprises.



Product: NetPilot Plus
Manufacturer: Equinet
Contact details: www.equinet.com/netpilot

NetPilot Plus from Equinet is Checkmark certified to AntiVirus Level 1. www.check-mark.com

The NetPilot Plus is basically a firewall, with AV functionality activated by a separate license. The appliance contained the most recent Sophos engine.

The management interface is clear, simple and attractive, with a wide range of configurable settings. Most of these need not be changed from the default.

Infected and unscannable emails can be discarded,

diverted to a specified account or (rather surprisingly) delivered to the intended recipient. It is not possible to disinfect attachments.

Reports list incoming viruses by name and quantity, but not the sender or recipient, or the time received. Logs can be emailed or viewed online.

Using the definitions of 22 August NetPilot Plus detected all the viruses in the June Wildlist.

THE VERDICT

The NetPilot Plus is a gateway appliance offering unified threat management with an easy-to-use management interface. Detection of viruses is accurate and reliable.



Juniper Networks NetScreen-5GT



DEVELOPER'S STATEMENT: For IT managers who need an advanced security appliance with superior price/performance and manageability to protect against all manner of network attacks.



Product: Juniper Networks NetScreen-5GT
Manufacturer: Juniper Networks
Contact details: www.juniper.net/products

NetScreen 5GT from Juniper Networks is Checkmark certified to AntiVirus Level 1. www.check-mark.com

The NetScreen-5GT is a compact device with an effective antivirus engine. An intuitive web interface allows very detailed control and quick navigation.

Access to the management interface is by login ID and password. Though only the administrator may log in, it is possible to add more than one administrator on a read-only or read-write basis.

The main menu in the web interface consists of clearly marked sections and subsections with easy to find and well grouped options. ScanManager enables the administrator to set auto update and decompression options and choose protocols to be scanned.

Using the definitions of 23 August, the NetScreen-5GT detected all the viruses in the June Wildlist without problems.

THE VERDICT

The NetScreen-5GT provides a wealth of features in a gateway appliance with a small footprint. The AV capability provides effective protection for common protocols.



BlackSpider MailControl AntiVirus



DEVELOPER'S STATEMENT: BlackSpider MailControl AntiVirus is a fully managed service providing enterprises with complete protection from viruses and malicious content hidden inside internet email.



Product: BlackSpider MailControl AntiVirus
Manufacturer: BlackSpider Technologies
Contact details: www.blackspider.com

MailControl AntiVirus from BlackSpider is Checkmark certified to AntiVirus Level 1.
www.check-mark.com

Traditionally, a customer has comparatively little input to a managed service such as this, but BlackSpider's MailControl AntiVirus is a little different. The client can choose to ignore the product, but a web console is also provided through which an administrator can make major changes.

The core of the console is Setup, which displays the default policy that governs how the service handles

traffic to and from the company. New policies can be added or the default can be edited from the many available options and features. Users can be linked into different groups with different actions for each group. The administrator may also generate reports for a given period, either a summary or a specific report.

MailControl AntiVirus detected all the viruses in the June Wildlist in on demand scanning without difficulty.

THE VERDICT

The MailControl managed service offers an administrator considerable control over the details of email policy while freeing him or her from the details of implementation.



SecurePipe Managed Network Security



DEVELOPER'S STATEMENT: SecurePipe delivers managed network security services. It helps clients strengthen security, reduce costs and improve compliance with regulatory requirements.



Product: SecurePipe Managed Network Security
Manufacturer: SecurePipe
Contact details: www.securepipe.com

SecurePipe Managed Network Security is Checkmark certified to AntiVirus Level 1.
www.check-mark.com

SecurePipe provides a series of devices that can be used as firewalls, but that are maintained not by the customer but by the company.

Customers must reconfigure their email servers so that outbound and inbound traffic is relayed to use SecurePipe's servers. This done, the responsibility for the transmission and safety of the SMTP traffic is SecurePipe's. This does remove the burden of

administration from a possibly overloaded employee.

There is a management interface for the customer to view via a web-based security console. Detailed logs are not available, but a display indicates the domains sending most email, the most frequent reasons for rejection and the recipients receiving most email.

SecurePipe detected all the viruses in the June Wildlist without difficulty.

THE VERDICT

SecurePipe offers a variety of managed network security services. Antivirus protection for email traffic is simple and quick to implement, requiring minimal reconfiguration.



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
- Beta testing and evaluation
- Custom testing ■ Certification
- Marketing your technology message to a global buying market

For full details of West Coast Labs' product testing, evaluation and certification services contact Mark Thomas, Sales Manager: rmthomas@westcoast.com



www.westcoastlabs.org

Contact information

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 Mark Thomas by email mthomas@westcoast.com • www.westcoastlabs.org