Corporate anti-virus software

Dave Mitchell looks at ten corporate anti-virus software solutions as well as the managed services route

Hardly a week goes by now without a virus causing mayhem, making anti-virus measures an essential part of a data-protection plan. The new breeds of viruses are a far cry from the boot sector and file infector varieties of a few years ago, as these mass-mailers are capable of causing untold damage and destruction. They can bring a company to its knees in a matter of days and in the process cost huge sums in lost business.

The nature of the virus has changed dramatically since the first examples were released into the wild over 20 years ago. A recent study by Network Associates even highlights parallels with biological viruses. Many attacks are seasonal, for instance – Christmas is a particularly bad time with a large number of email invites and jokes flying around. Points of origin and patterns of infection also bear close similarities – the majority of software viruses emerge in Asia and generally spread across the globe from east to west as each time zone starts its working day. It's clear that companies must protect themselves against this onslaught, and in this month's group test we bring together ten of the top anti-virus products designed specifically to protect networks.

Unlike the managed services route (*see p186*), the standard procedure for all these products is to place anti-virus utilities on each workstation and server. In most cases, the tools to manage them all are delivered from a central location. Local protection is provided by a real-time scanner, which keeps a close eye on all incoming and outgoing files and checks them first before allowing access. On-demand scanning facilities are also available, allowing users to run more in-depth checks on their files at scheduled intervals. Email protection is of paramount importance and these products will scan incoming and outgoing messages and attachments before passing them on.

It's worth noting that Outlook 2002 has basic built-in protection measures of its own for file attachments. Its Level 1 setting blocks access to a long list of file extensions including EXE, COM, SCR, VBS and BAT, and these settings can't be modified without the use of third-party applets. All other attachments are considered a Level 2 security risk and you're asked to save the file to the hard disk rather than opening it. However, the Level 1 setting can easily be overcome by renaming the file before sending it.

One feature common to nine of the anti-virus products on review is a complete reliance on a signature or definition file. This contains coding from each identified virus or worm to allow the scanning program to detect and identify the virus. However, this method means that vendors will always be on the defensive and can only ever react to a new outbreak rather than prevent it happening. This creates a chain of events that starts with the news of a new virus on the loose. The virus or worm then has to be captured and analysed, a new definition file created and posted on the vendor's website. Administrators then have to download and apply the file to every instance of the anti-virus software running on their network.

All products check for updates at regular intervals, but how often should this be set to run?

All products have the ability to check for updates at regular intervals, but how often should this be set to run? The Internet has broken down many barriers to viruses, as it offers fast delivery methods straight to your doorstep, most commonly via email.

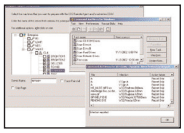
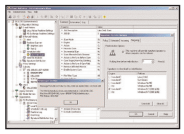
The bottom line is that until these update methods are changed to a more proactive solution, the majority of the anti-virus software vendors will never get ahead of the authors. Some large firms already have anti-virus software implemented, but are taking no chances by using a range of products to protect different levels of their network infrastructure. This approach is costly, but it can provide better protection should one vendor fail to respond to a threat or not update its software quickly. Another problem can become apparent on slower systems – the virus identity files are now so large the scanning process can have an adverse impact on general performance.

Reporting and notification need to be good as well so that potential threats to the network are highlighted and dealt with promptly. We found the level of responses to positive detection generally very good, although report details varied considerably.

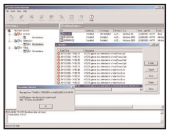
One particular user may be a regular, although not intentional, source of infection and if the software doesn't specifically identify them it could take weeks to locate the problem. The main thing to remember is the quicker a virus is dealt with the easier the clean-up operation will be. If the virus is isolated and contained within a single workstation, it will be just a matter of repairing the infected files where possible or deleting them and restoring from the latest backup copy. Either way, it's sheer folly for a company not to have any virus protection, but even if you do it's worth checking out the next few pages where you'll find plenty of information to help make your next buying decision.

FEATURE TABLE

PC PRO RECOMMENDED



	Command AntiVirus	CA eTrust Antivirus	H+BEDV AntiVir for Servers/ Workstations	Kaspersky Labs Corporate Suite	Network Associates McAfee Active Virus Defence	NetZ Computing InVircible	Panda Software Antivirus Enterprise Suite
Overall rating	★★★☆☆☆	★★★★☆☆	★★☆☆☆☆	★★★★☆☆	★★★☆☆☆	★★★★☆☆	★★★★☆☆
Price (per user exc VAT)							
10 users	£25	£23.30	£37.30	£32.80	£74.59	£50	£46.88
100 users	£17.50	£23.30	£17.70	£19.60	£49.89	£35	£29.87
Subscription period	1yr	1yr	1yr	1yr	1yr	1yr	1yr
Supplier	Command 020 7931 9301	Computer Associates 01753 577733	H+BEDV DatenTechnick online sales	Kaspersky Labs 0870 011 3461	Network Associates 0800 092 7160	Virus Defence Bureau 01844 277300	Panda Software 0870 444 5640
Manufacturer's website	www.command.co.uk	www.ca.com	www.hbedv.com	www.kaspersky.co.uk	www.mcafee.co.uk	www.invircible.com	www.pandasoftware.co.uk
SOFTWARE							
Management server	NT/2000	NT/2000/XP	N/A	NT/2000	NT/2000	95/98/ME/NT/2000/XP	NT/2000
SERVER SUPPORT							
Windows NT 4	✔	✔	✔	✔	✔	✔	✔
Windows 2000	✔	✔	✔	✔	✔	✔	✔
NetWare	Optional	Optional	Optional	✔	✔	✔	✔
Others	✖	✖	✖	Linux	✖	✖	✖
CLIENT SUPPORT							
Windows 95, 98, ME	✔	✔	✔	✔	✔	✔	✔
Windows NT, 2000, XP	✔	✔	✔	✔	✔	✔	✔
NetWare	Optional	Optional	Optional	✔	✔	✔	✔
Others	✖	✖	✖	Palm OS, Pocket PC, Symbian EPOC	Windows CE, Palm OS	✖	DOS, Windows 3.x
CLIENT/SERVER DEPLOYMENT							
Local	✔	✔	✔	✔	✔	✔	✖
Login script	✔	✔	✔	✔	✔	✔	✔
Network share	✔	✔	✔	✔	✔	✔	✔
Push from console	✔	✖	✖	NT/2000/XP	✔	✖	✖
Push from CD-ROM	✖	✖	✖	✖	✖	✖	✖
Multiple deployments	✔	✔	✖	✔	✔	✖	✖
Auto restart on completion	✖	✖	✖	✔	✔	✖	✖
FEATURES							
Remote management console	✖	✔	✔	✔	✔	✔	✔
Bootable installation CD-ROM	✖	✖	✖	✖	✖	✖	✖
Separate quarantine server	✔	✖	✖	✔	✖	✖	✖
Password-protect local settings	✖	✖	✖	✔	✖	✔	✔
Lock down local settings	✔	✔	✖	✔	✔	✔	✔
Allow client to run manual scans	✔	✔	✔	✔	✔	✔	✔
Allow client to scan network drives	✔	✔	✔	✔	✔	✔	✖
Other features	✖	✖	✖	✖	Desktop Firewall, ThreatScan	✖	PerimeterScan Firewall, PerimeterScan Proxy
SIGNATURE UPDATE METHOD							
Website download	✔	✔	✔	✔	✔	✔	✔
Scheduled downloads	✔	✔	✖	✔	✔	✔	✔
Manual downloads	✔	✔	✔	✔	✔	✔	✔
CLIENT UPDATE DEPLOYMENT							
Network – push	✖	✔	✖	✔	✔	✔	✖
Network – pull	✔	✖	✔ (Workstation)	✔	✖	✔	✔
Email	✖	✖	✖	✖	✖	✔	✖
Intranet	✖	✖	✖	✖	✖	✔	✖
Minimum update check interval	1min	1min	1wk	1hr	1hr	6hrs	1 day
ACTION ON POSITIVE DETECTION							
Deny access	✔	✔	✔	✔	✔	✔	✔
Clean	✔	✔	✔	✔	✔	✖	✔
Delete	✔	✔	✔	✔	✔	✔	✔
Quarantine	✔	✖	✔	✔	✔	✖	✔
Back up before delete/repair	✖	✔	✔	✔	✖	✔	✖
Modify name	✔	✔	✔	✔	✔	✔	✔
Log client off network	✖	✔	✖	✖	✖	✔	✖
Other	✖	Printer, Unicenter TNG	Local report file	✖	Printer	Report file	✖

	Sophos Anti-Virus	Symantec AntiVirus Enterprise Edition	Trend Micro OfficeScan/ ServerProtect
	★★★★★☆	★★★★☆☆	★★★☆☆☆
	£45	£63.38	£24.50
	£20	£46.55	£18.56
	1yr	1yr	1yr
	Sophos	Symantec	Trend Micro
	01235 559933	020 7616 5600	01628 400516
	www.sophos.co.uk	www.symantec.co.uk	www.trendmicro.co.uk
	NT/2000/XP	NT/2000/XP	NT/2000
	✔	✔	✔
	✔	✔	✔
	Optional	✖	✔
	✖	✖	✖
	✔	✔	✔
	✔	✔	✔
	Optional	✖	✔
	✖	✖	✖
	✔	✔	✔
	✔	✔	✔
	✔	✔	✔
	✖	✔	ServerProtect
	✖	✔	✖
	✔	✔	✔
	✖	✖	✖
	✔	✔	✔
	✖	✔	✖
	✖	✔	✔
	✖	✔	✔
	✖	✔	✔
	✔	✔	✔
	✔	✔	✔
	✖	✖	✖
	✔	✔	✔
	✔	✔	✔ (ServerProtect)
	✔	✔	✔
	✔	✔	✔
	✖	✖	✖
	✖	✔	✖
	✖	✔	✔
	1hr	15mins	1hr (ServerProtect)
	✔	✔	✔
	✔	✔	✔
	✔	✔	✔
	✔	✔	✔
	✖	✔	✔
	✔	✔	✔
	✖	✖	✖
	✖	✖	Printer (ServerProtect)

How we test

The most common method of testing anti-virus software is to use detection rates as a benchmark. However, test viruses used often call into question the validity of the results. It's debatable whether using simulated viruses is a suitable test, as most products should be able to recognise these as bogus and not flag them for attention. Rosenthal Utilities (**slonet.org/~doren**) offers a tool for creating a collection of fake viruses, but even the author points out that these are designed to be used for testing and validating security measures and aren't a replacement for the real thing.

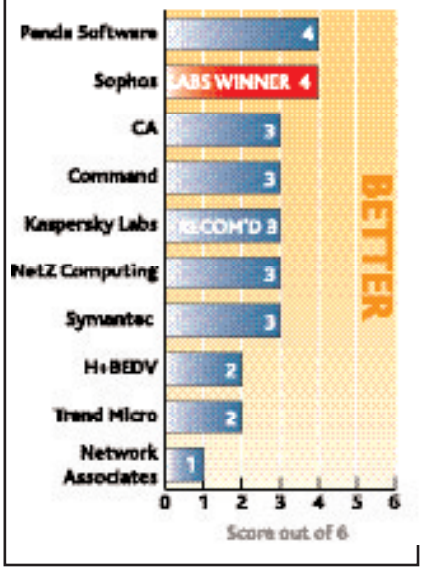
Rather than test detection rates, we feel it's more important to see each product's defences. In the home, a single PC will be at risk. In a network environment, the danger increases exponentially, so the software must offer the tools to efficiently and effectively block a potential infection in its tracks. To this end, we look at how each product responds to an infection attempt and what features it offers for clean-up operations. Alerting is also important, as administrators need to know the moment their network is exposed to a threat and what the software is doing about it.

All but one of the products relies on a signature or definition list to recognise viruses. This must be updated swiftly if the product is to be effective against the next identified threat, so we want to see how easy it is to download the latest updates and what automation is provided for deploying them speedily across the network.

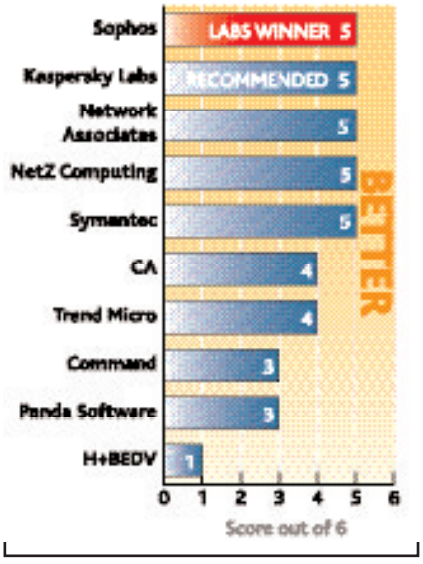
The testing environment is made up of five systems, with one running Windows 2000 Server and the others installed with Windows 2000 Professional, XP Professional, 98 SE and ME – all with the latest security patches and Service Packs. Each anti-virus product is initially installed on the server and then deployed to each system using the tools provided. All product updates and the latest definition files are downloaded, installed and deployed via a proxy server. External access is severed during testing. We introduce genuine viruses on the closed network, comprising Bugbear, Nimda, Badtrans, Loveletter and Magistr-B plus a couple of floppy disks infected with the old-timer boot sector baddies Form and V-Sign and watch how each product responds to their presence.

When choosing the best products, we take into account a number of areas. The software must be manageable and offer plenty of information about its current status such as which systems are protected, the nature of attacks and what the software is doing about them. Updates are also a key component to the software's effectiveness, so these must be easily accessible, simple to download and swiftly passed on to all systems.

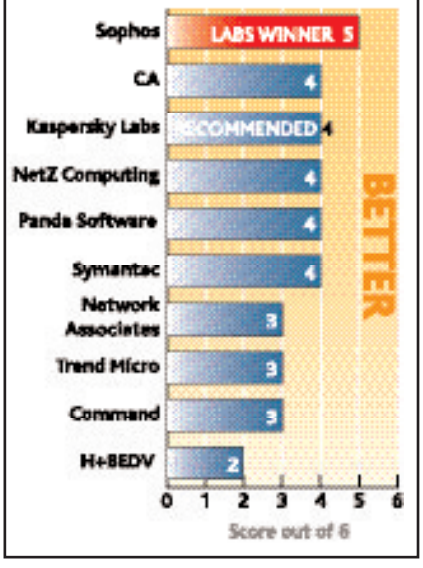
EASE OF USE



FEATURES



OVERALL

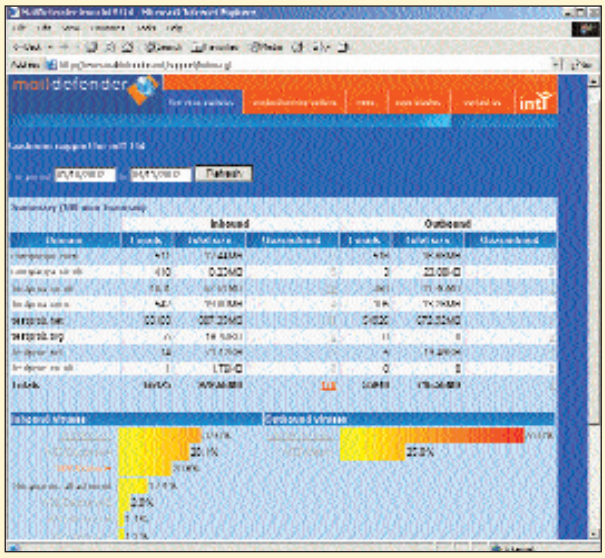


Managed anti-virus services

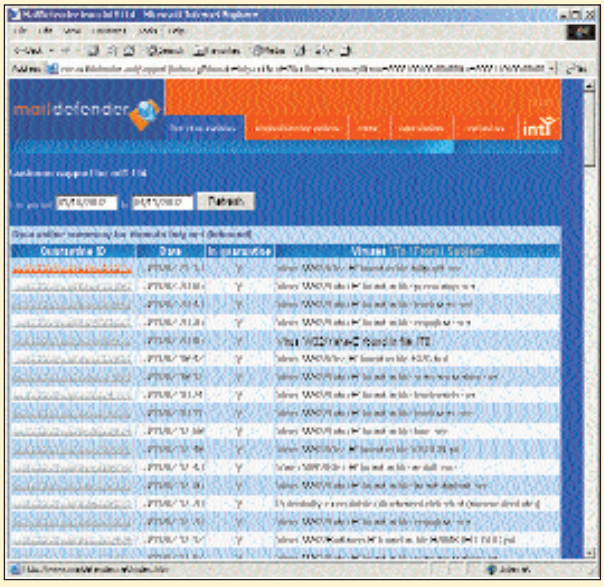
If the idea of adding the administration of anti-virus measures to your daily burden of chores doesn't appeal, how about passing some of the load on to a third party?

According to surveys conducted by ICSA Labs, 87 per cent of viruses were propagated using email during 2000. Surprisingly, this figure did drop slightly to 83 per cent during 2001, but this fall was partly due to the Code Red and Nimda worms, which can infect systems by other means than just email. Even so, it makes sense to place a higher priority on securing against this avenue of infection, and a number of companies have sprung up in response to this threat, offering a range of managed services primarily aimed at email and attachment scanning.

Bristol-based intY provides its MailDefender managed service, which is aimed at the small to medium-sized business. The company uses two separate data centres in London and Leeds, operated by Energis and GX Networks respectively. The hardware comprises rack-mount, Intel-based servers with sufficient built-in fault tolerance including mirroring to cope with a 75 per cent hardware outage. IntY also operates its own systems in Bristol, which can provide a reduced tertiary failover service if necessary.



Good web-based reporting tools keep you in touch with viral and quarantine action.



MailDefender allows you to drill down and view individual log entries to see who's receiving or sending viruses within your company.

Sophos' Anti-Virus software provides the primary defence against viruses and intY has an agreement with the company whereby it checks Sophos' website for new virus identity files every five minutes. A second scanning phase is provided by intY's own proprietary intYscan heuristic scanner, which it has developed over a number of years.

Installation procedures for MailDefender are minimal. You inform intY of your domain names and your ISP must be advised that mail to these domains is to be redirected to intY's servers. That's it, and the service should be up and running within 72 hours. Any mail directed to your domain now goes to intY's mail servers, where it's placed in a queue and unpacked ready for scanning. If Sophos Anti-Virus is happy with the contents, it's passed to intY's own scanning engine and then sent on to your ISP's mail servers for delivery. Outgoing email may also be scanned, and intY provides instruction on how to set your mail server up to send mail to the MailDefender service first.

In the event of a positive detection, the email and attachment are held back in a quarantine area for 30 days, pending your decision on what to do with it. After this period has expired, the file will be automatically deleted if no further action has been taken.

Notification options are plentiful, as messages can be sent to both sender and recipient, plus administrators, if an incoming message has been placed in quarantine. Infected outgoing mail is a little more sensitive, so MailDefender will quarantine it but only advise the sender of its actions. Performance is good and intY estimates that a 1MB email and attachment can be dealt with in less than two seconds.

Monitoring and reporting facilities are superb too, as MailDefender maintains an SQL database that logs all relevant email activity. Registered users may view general MailDefender activity from a standard browser and drill down to see statistics about their own company. This will allow you to view activity and alerts at the individual user level, so you can see which staff are most at risk and who's responsible for sending viruses.

At the time of review, there was a staggering ratio of one infected message to every 50 emails going through the MailDefender servers in a single 24-hour period.

For the small to medium-sized business, MailDefender looks a sensible alternative to in-house email scanning and can significantly reduce the burden for network managers. IntY's charges also look good value, as a 12-month contract for up to 50 users rounds out at £900, while £2,250 gets you a three-year contract for the same number of users.

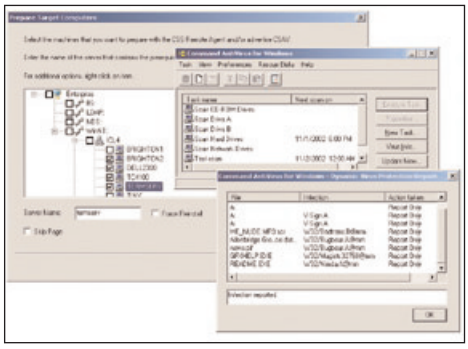
Contacts:
MailDefender www.maildefender.net
intY 0870 900 4689

Another company offering similar facilities is MessageLabs 01452 627627, www.messagelabs.co.uk

Command AntiVirus

PRICE 10 users, £25 each; 100 users, £17.50 each (all prices exc VAT)
SUPPLIER Command 020 7931 9301 INTERNET www.command.co.uk
VERDICT **Simple network deployment tools and good client protection, but minimal administration and alerting features.**

Command's anti-virus offering has seen a substantial spring clean this year, bringing in some long-awaited new features. Gone are the dusty help files that referred to the old F-Prot Professional utility on which AntiVirus was originally based, to be replaced by a CommandCentral utility that offers administrators some useful deployment tools.



One feature conspicuous by its absence is a management console, so once the software has been installed to your clients there are no tools for monitoring its progress. At the time of writing, Command was about to unveil its TotalCommand management tool, but this is aimed primarily at large enterprises and wasn't made available to us for review.

Even so, client deployment options are extensive, as CommandCentral allows you to create an MSI (Microsoft Installer) file where you can decide what components are installed and the settings for each function, whether users are able to scan local and network drives, and include predefined custom scan jobs. It then runs a full discovery scan of the network, so you can select the systems on which you want the Command agent installed. This lets clients run the central Anti-Virus installation routine either from a logon script or locally from the Run line.

Definition updates may be downloaded directly from the AntiVirus user interface or managed by CommandCentral. For the latter, you select a Command site, choose from definition files, component updates and upgrades and schedule the task to run at regular intervals. Note that this feature isn't compatible with proxy authentication, which must be disabled on the download system. The resultant files are then applied to the administrative installation points. The AntiVirus software contains an agent that checks the central image file for changes at logon and will automatically download any new files or modifications.

The local AntiVirus utility provides a comparatively basic interface, but does allow a variety of tasks to be carried out if the user has been granted permission. They can run on-demand and scheduled scans of their drives, allow scans to start after a specific period of inactivity and create a rescue disk set. However, without a central management console, there are few alerting options. AntiVirus can only create a local report, display a warning message or send an email to a single recipient.

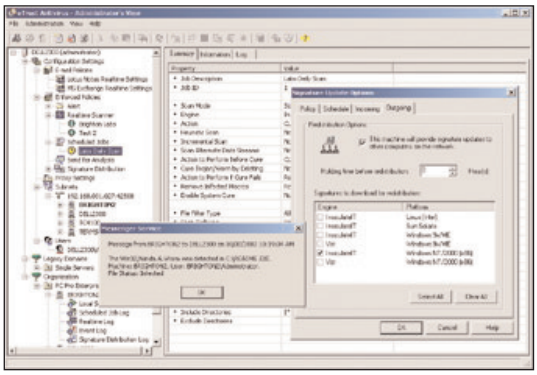
PC PRO RATINGS

EASE OF USE	★★★☆☆
FEATURES	★★★☆☆
VALUE FOR MONEY	★★★★☆
OVERALL	★★★☆☆

CA eTrust Antivirus

PRICE 10 users, £23.30 each; 100 users, £23.30 each (all prices exc VAT)
SUPPLIER Computer Associates 01753 577733 INTERNET www.ca.com
VERDICT **A reasonable price tag for a sophisticated software package that offers an intuitive management console and plenty of automation tools.**

This latest version of CA's virus-protection package revolves around its InnoculateIT software and an administration console. This offers a range of new features, including improved discovery and a web-based interface. The suite comprises three main components – an administration server along with the local on-demand and real-time scanners.



Deployment tools are more limited, as installation to NT, 2000 and XP systems is automated, with a separate remote installer that uses an installation command file (ICF) to deploy the same group of Registry settings to multiple systems. However, as with Kaspersky, clients running Windows 95, 98 or ME can only be deployed using a login script associated with the setup files in a shared directory.

The entire eTrust environment may be managed from the server running the administration component. A network view based on IP subnets will discover and display all systems that have the eTrust software installed. Systems are managed by placing them into containers that can be used to represent logical or physical views of the network. To add a system to a container, it must first be authenticated. This is problematic for Windows 95, 98 and ME systems, as user accounts are managed locally, so a DOS utility is used to create a special authentication file.

Policies control how systems run the software and react to infections and, once assigned, they can be locked down to prevent users modifying the settings. Policies are also used to schedule regular on-demand scans and distribute new virus signature files, although for the latter there are minimal control options. The supplied quarantine rules apply to users and not files, so you can block network access to a system with an infected file for a specific period.

Users will find a new icon in the System Tray indicating the real-time scanner is active. They can view and modify its configuration, but if central settings have been applied and locked down they'll find the OK button has been greyed out. A local copy of eTrust InnoculateIT is also installed, allowing users to run their own on-demand scans. Alerting has always been a strong point of eTrust products, and the Alert Manager service supports masses of notification options that can be applied separately to the on-demand and real-time scanners.

PC PRO RATINGS

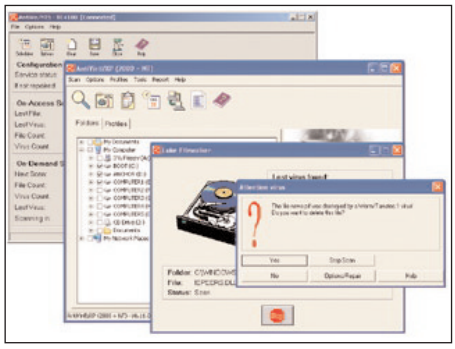
EASE OF USE	★★★☆☆
FEATURES	★★★★☆
VALUE FOR MONEY	★★★★☆
OVERALL	★★★★☆

H+BEDV AntiVir for Servers/Workstations

PRICE 10 users, £37.30 each; 100 users, £17.70 each (all prices exc VAT)
SUPPLIER H+BEDV DatenTechnik online sales INTERNET www.hbedv.com
VERDICT **A collection of utilities with no real integration and minimal management facilities, making the AntiVir solution a poor choice for protecting networks.**

AntiVir may not be well known in the UK, but on the surface it offers an impressive selection of anti-virus tools for a wide range of platforms, including options for NetWare and Exchange. However, dive beneath and you'll find a disparate collection of utilities with minimal management features and little or no integration between components.

AntiVir for Servers looks after Windows NT and 2000 Server platforms and installs a real-time scanner as a service, which is completely transparent. To access its settings, you load the AntiVir remote-control console. This offers a basic interface revealing configuration settings along with real-time and on-demand scan status. A scheduler allows automated scans to be run at regular intervals on selected drives or directories. However, notification and alerting options are poor, as these are limited to a network broadcast to specific systems, an entry in the NT event log and a locally held report file. Automating virus definition updates proved to be a mystery too. We could find no tools for this, the documentation was devoid of instructions and our calls for help went unanswered by the AntiVir support staff.



Remote management of other servers is also a possibility – you select a system from the remote console, although this doesn't differentiate between servers and workstations and will fail if the target is already running the console locally. You get the same interface, except that all scanning and scheduling commands are being sent to the remote system and you can remotely monitor their progress.

AntiVir for Workstations comes in two varieties, with one for Windows NT, 2000 and XP and another supporting Windows 95, 98 and ME. Note that there are no central deployment and management facilities and no integration with the server remote console, so users are largely responsible for their own local protection. The interface is easy enough to use and offers plenty of scanning tools, although calling the main file scanner utility 'Luke Filewalker' is rather juvenile.

Definition update options are more sophisticated than those in the server version, as one workstation can download them from the AntiVir website and place them in a shared directory where other systems are able to pull the updates over the network at regular intervals.

PC PRO RATINGS

EASE OF USE	★★☆☆☆
FEATURES	★☆☆☆☆
VALUE FOR MONEY	★★☆☆☆
OVERALL	★★☆☆☆

Kaspersky Labs Corporate Suite

PRICE 10 users, £32.80 each; 100 users, £19.60 each (all prices exc VAT)
SUPPLIER Kaspersky Labs 0870 011 3461 INTERNET www.kaspersky.co.uk
VERDICT **This huge toolbox of anti-virus measures looks good value. It comes with sophisticated management and deployment tools, but alerting features could be better.**

At first glance, Kaspersky Labs' Corporate Suite looks to offer top value, as it includes virtually every anti-virus tool most networks are likely to need, as well as support for Linux, Exchange and Lotus Notes. Not only that, it brings them all together under a single Network Control Centre (NCC) management utility. The interface is initially quite daunting, but it allows you to create groups to represent your logical network, with each group requiring a control server to look after all included workstations.

PC PRO RECOMMENDED

Workstation and server deployment is simple – you add one of the supplied predefined packages to the NCC, check all the workstations in the network view alongside that are to receive it and run the job. However, you can only push anti-virus programs to NT, 2000 and XP systems – 95, 98 and ME must have the software deployed locally or via a login script. From the NCC, you're able to monitor individual systems, modify their settings and remotely run manual scans on multiple workstations simultaneously.

Automatic definition updates are a little trickier to set up, but once again there are plenty of options, because the management server is used to download updates from the Web. You can then either push the software to groups of workstations or allow them to pull it from the server at regular intervals. Program updates are dealt with in a similar manner, and a separate quarantine area may be created on the server to which dubious files are sent.

Workstation users can be allowed to interact with the local copy of the software, but transparency isn't an option, since Kaspersky insists on installing different utilities for scanning, updating, monitoring and scripting. If a workstation is in trouble, its icon changes to warn you, but notification options are probably the weakest area of the Corporate Suite. Warning messages are limited to a network broadcast and email, and the contents of the messages generated aren't overly informative – they don't even state what virus caused the alarm. However, a wide range of extra features make up for this, with tools such as virus outbreak monitoring supported as standard, whereas companies like Trend Micro expect you to pay more for this.

PC PRO RATINGS

EASE OF USE	★★★☆☆
FEATURES	★★★★★
VALUE FOR MONEY	★★★★★
OVERALL	★★★★☆

Network Associates McAfee Active Virus Defence

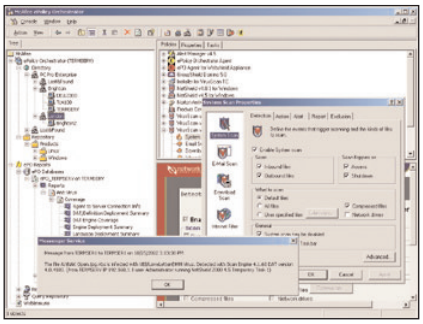
PRICE 10 users, £74.59 each; 100 users, £49.89 each (all prices exc VAT)
SUPPLIER Network Associates 0800 092 7160 INTERNET www.mcafee.co.uk
VERDICT **A wide range of tough security features that includes firewall protection, but muddled documentation and awkward installation and management procedures won't impress.**

It's one of the most comprehensive security products on review, but Active Client Security Suite proved difficult to install and manage. Nine separate manuals and no overview of how they interact with each other doesn't get things off to a good start. Also, the fact that the ePolicy Orchestrator central management software is supplied on a disk for managing thin clients is confusing.

The management software comprises a server and console, and all systems to be included need a small agent utility installed locally. Groups organise your network into manageable chunks and the agent and anti-virus software may be deployed at the group level or to individual systems.

With the agent in place, you can monitor each system from the console, view basic hardware details, deploy other software packages and enforce anti-virus policies. The main interface is similar to Symantec's, but doesn't offer the same tight integration with each managed product. You can't initiate an immediate manual scan of single or multiple clients with a few mouse clicks.

WebShield and VirusScan provide server and workstation protection respectively and offer a similar level of tools to the real-time scanner provided in McAfee's well-respected desktop product. For workstations, there are options for system, email and download scanning, and you can also block access to lists of website URLs and IP addresses. Prior to deployment, you browse through a list of these features and decide which ones to allow the client to access. Unfortunately, automating download and deployment of signature updates proved awkward to



configure – this should be far better documented, considering the software supplied for review was nine months out of date and desperately needed updates.

Alert Manager takes some beating, as it offers an extensive range of tools for sending warnings to a wide variety of destinations. This software suite is the most expensive on review, but, in time-honoured fashion, McAfee can't resist bundling in extra products. You get VirusScan for handheld devices, ThreatScan for identifying security loopholes and a complete desktop firewall solution that can also be managed centrally from the same console.

PC PRO RATINGS

EASE OF USE	★☆☆☆☆
FEATURES	★★★★★
VALUE FOR MONEY	★★☆☆☆
OVERALL	★★☆☆☆

NetZ Computing InVircible

PRICE 10 users, £50 each; 100 users, £35 each (all prices exc VAT)
SUPPLIER Virus Defence Bureau 01844 277300 INTERNET www.invircible.com
VERDICT **A unique network anti-virus solution that doesn't require constant updates. It offers comprehensive management tools and the price includes assisted installation.**

InVircible stands out from the crowd partly due to its longevity – it was originally developed for the Israeli military in the early 1990s. However, what makes it even more unique is it doesn't rely on definition files – it's designed to look purely for virus-like behaviour. True, some vendors offer a heuristic scan mode, but InVircible is the only product of this type we've seen work.

For example, it checks scripts irrespective of their entry point and uses a weighting system that determines whether the code is malicious. The fact that it's a script scores against it, but if it tries to access an address book InVircible will simply stop it functioning. The same applies to macro viruses, as InVircible will look at the commands and decide whether they're attempting a dubious manoeuvre. The biggest advantage is that InVircible doesn't rely on downloads to allow it to recognise a new threat and is one of few proactive anti-virus products.

Installation isn't helped by a lack of good documentation, but this is because the price includes full on-site assistance for this phase. Clients are deployed with a logon script, and different scripts may be used to determine what access, if any, clients can have with the local Interceptor utility. An administration utility that can run on any version of Windows provides a comprehensive management interface where it's possible to view protected systems, check on viral activity, remotely run commands or programs on other systems and download and deploy software updates.

InVircible reacts differently to an infection, as, by its nature, it doesn't know or care what type of virus it has found, so it won't attempt to clean a file. It's designed primarily to offer complete transparency and will deny access, delete or rename the file and log the suspect user off the network if required. This philosophy also means reporting is kept to a minimum – InVircible will just send a broadcast and produce a report detailing its actions. Executable files may be restored using the Audit and Integrity Expert, as this takes a snapshot of critical information and uses it to return an infected file back to its original state.

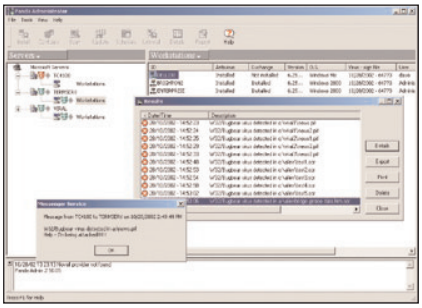
PC PRO RATINGS

EASE OF USE	★★☆☆☆
FEATURES	★★★★★
VALUE FOR MONEY	★★☆☆☆
OVERALL	★★★★☆

Panda Software Antivirus Enterprise Suite

PRICE 10 users, £46.88 each; 100 users, £29.87 each (all prices exc VAT)
SUPPLIER Panda Software 0870 444 5640 INTERNET www.pandasoftware.co.uk
VERDICT **A choice range of features for the price, with good centralised administration, but documentation could be better and notification options are limited.**

Although not that well known in the anti-virus market, Panda Software is gaining plenty of respect with a range of products that offers extremely good value. Its Antivirus Enterprise Suite is no exception – it comes packed with features, including Panda's PerimeterScan utility for firewall and proxy servers, plus excellent mail server support.



The action starts at the central Administrator console, which is designed to deploy and manage all the anti-virus components. Installation is swift, although some areas of the manual are confusing. It indicates that the console can run on Windows 9x and ME systems, whereas this is only applicable to systems that have the Novell Client installed and are managing NetWare servers only. The online help is also unfinished and offers no search facilities.

All available servers are displayed in the main window, with another to the right for workstations, and the views can be swiftly customised to show only specific operating systems. Servers may have the anti-virus components deployed immediately, but workstations will only appear once they have the software installed. These are loaded as packages for each required OS and can be deployed either by a login script for Windows domain members or by running the RINSTALL utility locally from a network share for workgroup members.

The console allows global parameters to be applied, so you're able to decide what parts, if any, of the local AntiVirus Platinum software users are allowed to play with. It's also possible to spread the management load over a number of servers, as each will look after associated workstations and manage their scan settings.

Signature updates are easily downloaded and the process can be scheduled, although Panda Software only updates its website once a day. Clients are set up to contact their management server at regular intervals to check for and retrieve any new files. Panda had no problems in blocking our virus attacks, but we found its responses were limited. When a virus is spotted, the Panda icon next to the relevant group turns red, but notification options are among the weakest here. Panda can only deliver a network message to one system or an email warning to a single recipient in the event of a positive detection.

PC PRO RATINGS

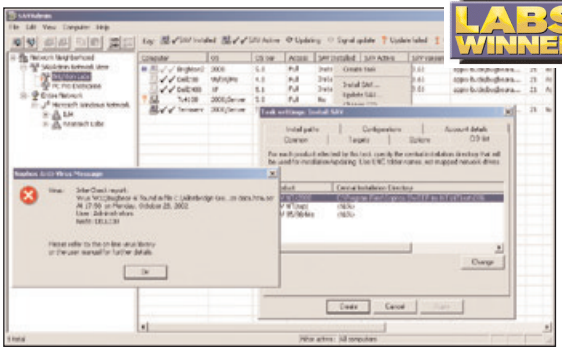
EASE OF USE	★★★☆☆
FEATURES	★★★☆☆
VALUE FOR MONEY	★★★★☆
OVERALL	★★★★☆

Sophos Anti-Virus

PRICE 10 users, £45 each; 100 users, £20 each (all prices exc VAT)
SUPPLIER Sophos 01235 559933 INTERNET www.sophos.co.uk
VERDICT **Good value with high levels of protection, minimal impact on local and network performance, plus new and improved management tools.**

PC PRO LABS WINNER

Traditionally, Sophos has concentrated on protecting networks rather than single users and, as a consequence, offers a number of features not found in competing products.



Its Anti-Virus product is built around a locally installed InterCheck utility that scans all files on access and adds a checksum for each one to a locally held list to denote it's clean. Any subsequent accesses to authorised files don't require the scanning process to be started again, so workstation overheads are reduced considerably. Only if a file is updated or if new ones are copied or created on the workstation will InterCheck verify them first.

All users see is a small InterCheck Monitor icon in the System Tray that allows them to view current anti-viral activity and a log file. The advantages of this method are almost total transparency and a minimal impact on local and network performance.

The SAVAdmin utility provides a tidy management interface from where the client software can be deployed to other servers and workstations using a central installation point and login script. It can auto-detect new systems and deploy the software automatically, but requires an agent to be installed locally to monitor Windows 95, 98 and ME systems. A separate Auto-upgrade feature checks each user's workstation when they log on and downloads and applies any program updates and new virus identification files that are held on the central server.

Each user gets their own copy of Anti-Virus Sweep to play with, but the main interface hasn't been changed for many years now. However, it's simple for users to select drives for on-demand scans or to schedule a scan for regular intervals.

Deployment of Sophos' virus identity files and program updates has been made easier with the new Enterprise Manager, as this MMC snap-in is designed to run scheduled and manual downloads from Sophos' secure website and automatically deploy them across the network. Reactions to a positive detection are plentiful, and Anti-Virus can shred infected files by overwriting their physical location so they can't be recovered. Reporting is also reasonably good. Anti-Virus is able to send network broadcasts to specific users or systems, email messages to any number of recipients and generate SNMP events.

PC PRO RATINGS

EASE OF USE	★★★★☆
FEATURES	★★★★★
VALUE FOR MONEY	★★★★★
OVERALL	★★★★★

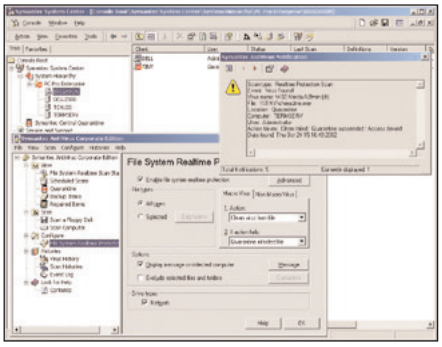
Symantec AntiVirus Enterprise Edition

PRICE 10 users, £63.38 each; 100 users, £46.55 each (all prices exc VAT)
SUPPLIER Symantec 020 7616 5600 INTERNET www.symantec.co.uk
VERDICT **An enterprise solution with a price tag to match, but you do get excellent centralised management and impressive alerting and quarantining tools.**

Central to Symantec's enterprise security software is System Center, which provides a remote console from where a variety of anti-virus products are managed. It installs as an MMC snap-in to which you add further modules, depending on the products you wish to manage. Once the Norton AntiVirus snap-in is loaded, you arrange your anti-virus servers into groups according to how you want to manage your clients. Each server group requires a primary server that manages the configuration and tasks for the group and may be used to deliver new signature updates.

Installation is a lengthy but well-documented process, and System Center can populate groups automatically, as it runs a network discovery routine over both IP and IPX. Groups are easily modified by dragging and dropping servers into a different group, and all associated clients will be carried across with the server. Local protection for servers and clients is handled by the network version of Norton AntiVirus, which is easily deployed from the System Center console. A real-time scanner is permanently loaded in the background and takes its instructions from a primary or secondary server. There are plenty of scan options, and files may be sent to a Quarantine server, which requires another MMC snap-in before it can be managed remotely.

Deploying scanning rules to multiple systems is simple – right-click on a group or server and select either the server or client real-time scan options. Your choices are automatically sent to the relevant systems. It's possible to lock out attempts to unload or uninstall the software and request a password before a user can scan a network drive.



Symantec's team of LiveUpdate and VDTM (virus definition transport method) regularly downloads updates and pushes them to clients, although we found this partnership difficult to set up and poorly documented. Alerting, on the other hand, is particularly impressive. Symantec's AMS2 keeps you in touch with the action, sending out a wide variety of warnings if viral activity is detected or if any problems with the anti-virus software itself are identified. Customised messages may also be created and it's possible to associate more than one alert action with an event.

PC PRO RATINGS

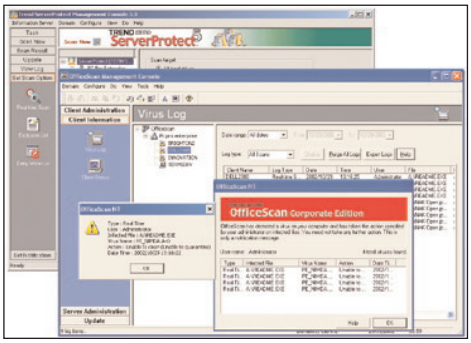
EASE OF USE	★★★☆☆
FEATURES	★★★★★
VALUE FOR MONEY	★★★☆☆
OVERALL	★★★★☆

Trend Micro OfficeScan/ServerProtect

PRICE 10 users, £24.50 each; 100 users, £18.56 each (all prices exc VAT)
SUPPLIER Trend Micro 01628 400516 INTERNET www.trendmicro.co.uk
VERDICT **A wide range of protection tools at a low price, but the differing levels of features and two separate management consoles for workstations and servers add unnecessary complications.**

Trend Micro takes a two-pronged strategy against viruses – OfficeScan looks after workstations, while ServerProtect guards your Windows and NetWare servers. The biggest drawback of this approach is the need to install two disparate products and manage them using two separate consoles. This wouldn't be a major problem if the consoles were similar in design, but their lack of consistency is confusing.

Both products are simple to install and can create shared installation points for deployment using network shares and login scripts. OfficeScan requires a server to act as a central administration point, which can be running NetWare as well as Windows NT or 2000. From here, you're able to select multiple systems and swiftly deploy the client software across the network. Users get an OfficeScan utility for local use, and administrators can lock it down or allow access to specific scan settings.



Notification options are severely limited – all you get is a network message and a modified icon in the console for the relevant client. If you want features such as email, pager and SNMP trap support, you need to purchase Trend's optional VCS package. You may opt for web or file server-based versions of the management console, but we found that the latter has no option to automate definition updates, so they need to be downloaded and applied manually to each group of users.

The ServerProtect version kicks off by installing an Information Server to act as a central administration point. You then deploy Normal Server packages to the remaining systems. There are some similarities with the OfficeScan console, as all systems are neatly arranged in an Explorer-style tree structure and it's possible to view system attributes opposite.

However, far more features are on offer. You can select individual systems and run remote scans, create schedules to fully automate updates, and even select remote directories and files from the ServerProtect console and deny write access to them. Tasks are used exclusively to automate procedures and provide plenty of Wizard-based help to create schedules. Standard notification options are also far superior to OfficeScan, including email, pager activation via a modem and even a printed warning.

PC PRO RATINGS

EASE OF USE	★★☆☆☆
FEATURES	★★★★☆
VALUE FOR MONEY	★★★★☆
OVERALL	★★★☆☆