WORDS: TERENCE GREEN **ILLUSTRATION:** RD2_MEDIA

Damage limitation

Viruses are a fact of life – just when you think you're safe, another one rears its ugly head, so anti-virus software is a must. We test 10 products to ensure you keep infection at bay

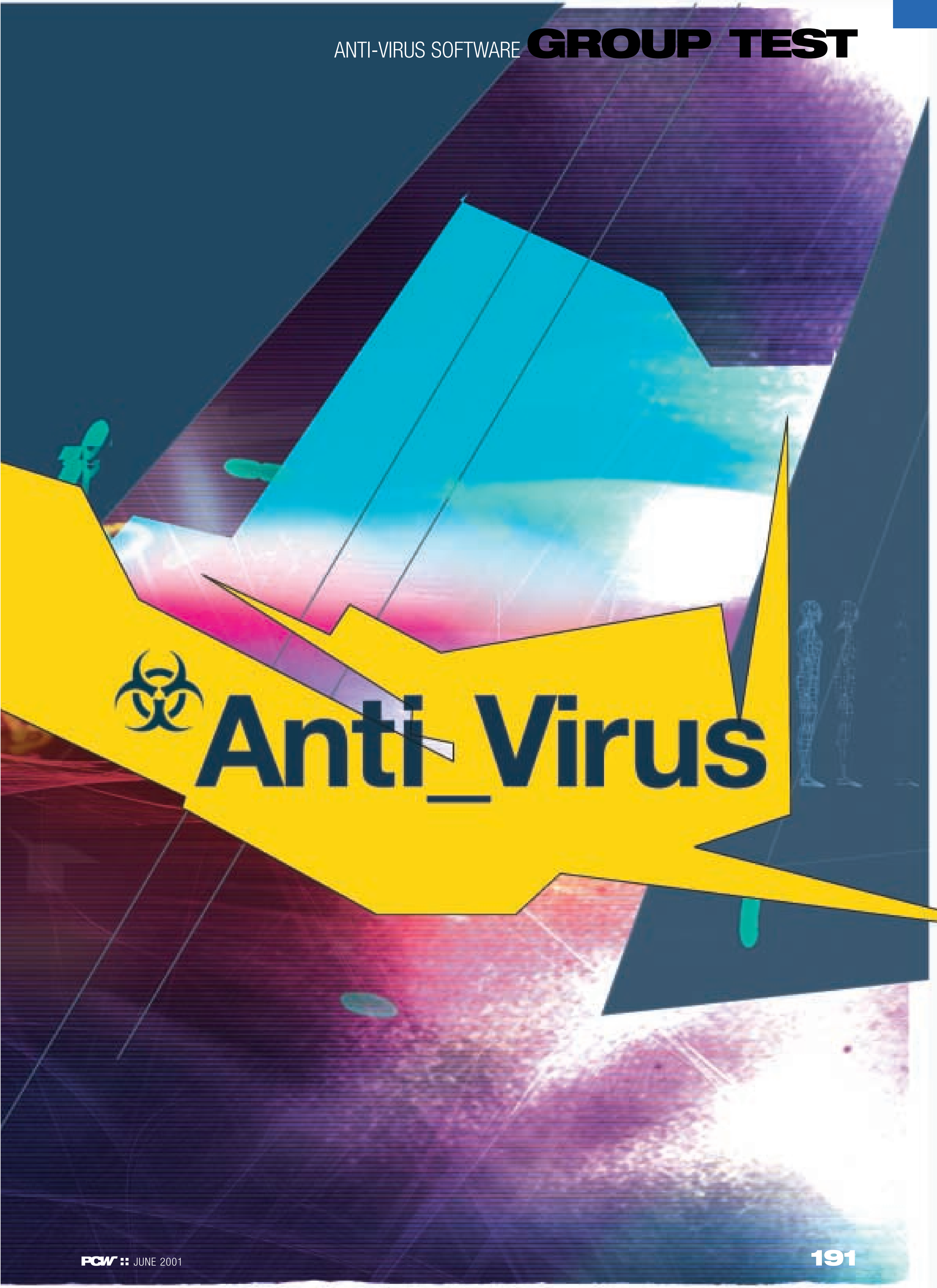
Two days before Valentine's Day another new computer virus made the headlines. It arrived as an attachment purporting to be a picture of tennis player Anna Kournakova. If opened it attempted to send the virus to everyone in the Outlook address book. Like many recent attacks, this one relied on social engineering and the prevalence of Outlook or Outlook Express to spread rapidly.

Until a few years ago computer virus attacks rarely made the news. Most anti-virus vendors have been careful to avoid raising virus fears in the wake of the great fiasco of 1992, when a virus set to trash hard disks on 6 March, Michelangelo's birthday, made world news. After a computer vendor announced that it had accidentally shipped 'Michelangelo' on a batch of computers, a couple of anti-virus software vendors made some rash claims about the risk. The news media printed stories putting millions of computers at risk and the world held its breath as 6 March arrived; and nothing happened.

Ever since 'Michelangelo' many people have believed virus scares to be a combination of scare marketing and misinformed reporting. Sadly, attacks like 'Melissa' and 'Love Letter', to use their common names, are very real and cause real damage, mainly because so many people are now online, exchanging email and visiting websites. Even sadder, much of the damage is preventable, but protection is not as simple as being ultra-careful about email attachments, making Outlook/Outlook Express more secure, or using an anti-virus scanner and keeping it updated. All of these help, but true security can never be guaranteed while people are involved in the process. An anti-virus scanner should never be your only defence but it should be an essential part of your security measures. To help you get the one that's right for you, we compare 10 top anti-virus products for Windows.

>

CONTENTS


Anti_Virus

Command
Anti-Virus Version 4.60

PRICE £58.69 inc VAT **CONTACT** Command 020 7931 9301 www.command.co.uk
SYSTEM REQUIREMENTS Windows, 8MB of RAM, 9MB hard disk space
PROS Easy to use; support for NetWare clients **CONS** A little limited in scanning options
OVERALL Easy to use; aimed at the corporate market
SCORE ■■■□□

Command Anti-Virus is easy to install and straightforward to use. The user interface is plain but slightly dated in comparison to some of the other products here, but it's very usable and provides a good level of protection.

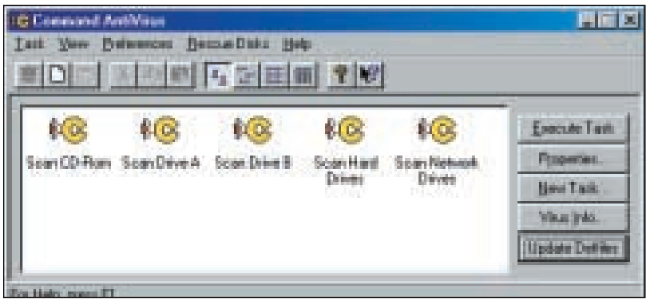
Based on the F-PROT scanning engine it provides on-access, on-demand and command-line scanning with Rescue disks. It supports DOS, Windows 3, 95, 98, Me, 2000 and NT Workstation and Server, Microsoft Exchange and Lotus Notes.

Command also supplies the management utility CSS Central, which a system administrator can use to automate scanning, scheduling and updating for networked computers. A NetWare agent for Novell networks is available. Since not all anti-virus clients work with the NetWare 32 client this is a benefit.

Installation is easy and setting scan parameters simple as there are minimal options. The basic scanning tasks are preset, but you can add customised scanning tasks for particular file sets, perhaps for an attachments directory or for quick scans of document files. Scans can be started manually or scheduled for a regularly time. An icon in the Windows Taskbar provides quick access to scanning and configuration.

Command doesn't scan inside Zips by default so you have to tell it to do this and run a manual scan. It's all very easy but we did experience an upset when Command choked on a PowerPoint slideshow. The system ground to a halt. Excluding PowerPoint slideshows from deep scans, a few quick clicks fixed it for the future.

On-access scanning options are limited – on or off, executing files and memory – with none of the flexibility in other scanners that allow you to select to scan on file writes, as well as file opens. But it's easy to enable and disable without rebooting. Command works well and its F-PROT engine is one of the better ones, but the program is looking a little long in the tooth against the more modern-looking opposition.



Basic scanning tasks are preset but you can tailor Command Anti-Virus to scan other file sets

Computer Associates
InoculateIT Personal Edition 5.2.5

PRICE Free **CONTACT** Computer Associates http://antivirus.cai.com
SYSTEM REQUIREMENTS Windows, 8MB of RAM, 4MB hard disk space
PROS Small; daily updates; fast **CONS** Must reboot to enable/disable on-access scanning
OVERALL Unbeatable value! Excellent introduction to anti-virus technology
SCORE ■■■■□

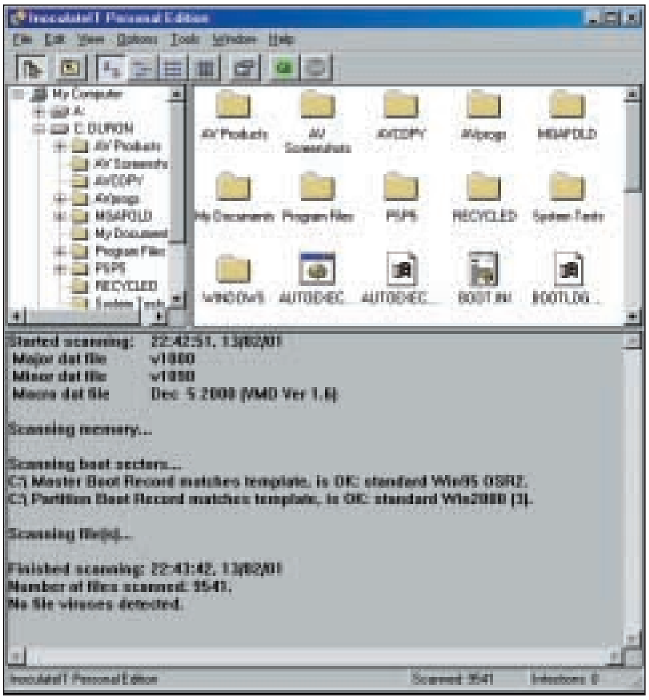
InoculateIT Personal Edition runs on Windows 98, 95, Me, 2000 and NT Workstation, only takes up 4MB of space on your disk, and is fast. It's free for personal use and registration entitles you to free updates and upgrades. Email support is also free and when we tested it out, a response arrived within the working day.

InoculateIT PE can only be downloaded from the Internet and Computer Associates is obviously giving this product away as a taster for its paid-for products, but it's good and works well for the average home user. If you like it, buy it, but you don't have to, and you'll have learnt more about the type of product you do want. Unlike most free evaluations you can download both upgrades of the scanner software and new virus signatures. Unusually, InoculateIT was one of the first scanners to provide daily updates.

You can't expect too much from a free scanner so there's no scheduler and updates are done manually, but a timer can be set to warn you on a regular basis. Then it's simply connecting to the Internet and clicking on the AutoDownload button and the rest happens automatically.

InoculateIT attempts to detect and clean infections and can be set to do so automatically or to prompt first. InoculateIT also resembles its paid-for brethren in using 'heuristic' techniques to detect unknown viruses by looking for suspicious activity. All virus scanners will inform you of such activity but differ in how it's handled. A high-class scanner will quarantine the file giving you a chance to update your virus signatures and to retest it, but with InoculateIT such incidents are handled manually.

If you think you need to open an attachment, normal practice is to move it to a folder set aside for the purpose and to recheck it after maybe a week, having updated your signatures in the meantime. The biggest hassle is rebooting to switch realtime protection on and off, but you shouldn't be doing this often.



```
Started scanning:   22:42:51, 13/02/01
 Major dat file     v1000
 Minor dat file     v1000
 Macro dat file     Dec 5 2000 (VMD Ver 1.6)

Scanning memory...

Scanning boot sectors...
C:) Master Boot Record matches template. Is OK: standard Win95 OSR2.
C:) Partition Boot Record matches template. Is OK: standard Win2000 [3].

Scanning file(s)...

Finished scanning: 22:43:42, 13/02/01
Number of files scanned: 9541.
No file viruses detected.
```

It's not the most comprehensive, but it's free, doesn't take up much space and you get efficient email support

F-Secure
Anti-Virus version 5.21

PRICE £84.60 inc VAT **CONTACT** F-Secure 01223 478 800 www.f-secure.com
SYSTEM REQUIREMENTS Pentium, Windows, 32MB of RAM, 25MB hard disk space
PROS Double-strength scanning; virtually transparent **CONS** No standalone scheduling
OVERALL Good standalone, but even better on a network
SCORE ■■■□□

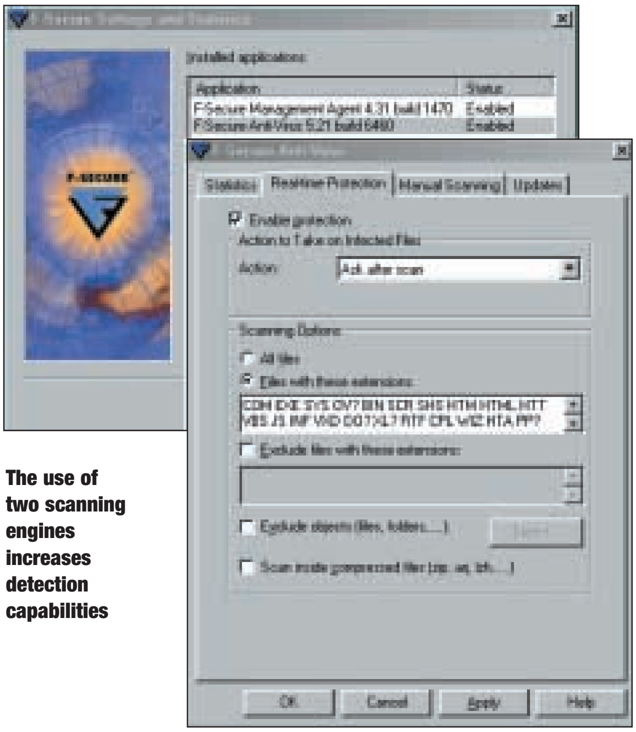
F-Secure is an unusual anti-virus product, as it uses two different anti-virus scanning engines – the F-PROT and the AVP from Kaspersky Anti-Virus (KAV). A third, the new Orion scanning engine is available on Windows 2000 but not 98.

By using two engines F-Secure increases its detection capabilities and minimises the likelihood of detecting false positives. The downside appears to be that manual scans take longer to complete, especially when F-Secure is asked to scan inside compressed Zip files. Normally, when used in its default 'smart' settings, Zips aren't scanned and, although F-Secure did display a slightly larger performance hit during testing, it was within reasonable expectations.

The question of scanning inside Zips is contentious anyway, since an archived file by definition isn't a threat. It may contain a threat, but it's not activated until it's released from the archive. Many people believe that's the time to scan for viruses. If so, the combined strengths of the F-PROT and AVP engines should provide more than adequate detection power to capture most suspicious activity with realtime monitoring. Incidentally, F-Secure detected 'Kournakova' with the AVP engine while other scanners based only on F-PROT missed it.

Although an excellent anti-virus tool, F-Secure isn't really a standalone user product. F-Secure is designed to run silently in the background, reporting problems to the network administrator and cleaning up problems automatically. It has excellent network management, two scanning engines, a very clean user interface, and a 'Disinfection Wizard' that fixes infected files easily. It works well as a standalone system but the network orientation means it doesn't include a scheduler. Standalone users can configure the files to be scanned and the action to take when a problem is discovered, and that's about it, apart from downloading updates.

In addition to Windows 98, this product supports 95, 2000 and NT4. Earlier versions are available for DOS, OS/2, Windows 3, and NT 3.5.


Installed applications:

Application	Status
F-Secure Management Agent 4.31 build 1470	Enabled
F-Secure Anti-Virus 5.21 build 6480	Enabled

☑ Enable protection
Action to Take on Infected Files
Action: Ask after scan
Scanning Options
○ All files
● Files with these extensions:
COM EXE SYS OV? BIN SCR SHS HTM HTML HTT VBS JS INF VXD DO? XL? RTF CPL WIZ HTA PP?
□ Exclude files with these extensions:
□ Exclude objects (files, folders, ...)
□ Scan inside compressed files (zip, arj, lzh, ...)

The use of two scanning engines increases detection capabilities

Frisk Software
F-PROT for Windows

PRICE $25 (£17) online **CONTACT** Frisk Software +354 561 7273 www.complex.is
SYSTEM REQUIREMENTS Windows, 4MB of RAM, 4MB hard disk space
PROS Fine-grained control for advanced users **CONS** Lacks bells and whistles
OVERALL No frills but all the essential features
SCORE ■■■■□

F-PROT for Windows dates back to 1989. It was one of the original anti-virus scanners and the first to use heuristic scanning. Since then the F-PROT development team has worked with various companies such as Command and F-Secure, while continuing to develop F-PROT technology.

The latest version 3.08c, at the time of writing, is available as a DOS scanner and wrapped into a Windows package, which includes the DOS version, plus Windows-based on-demand, on-access and macro scanning. This Windows version (FP-WIN) can also run on Windows emulations. The DOS version is free, while the Windows version costs $25 (£17) for personal use and can be purchased online. For your money you get free updates and program upgrades for one year. A trial version times out after 30 days.

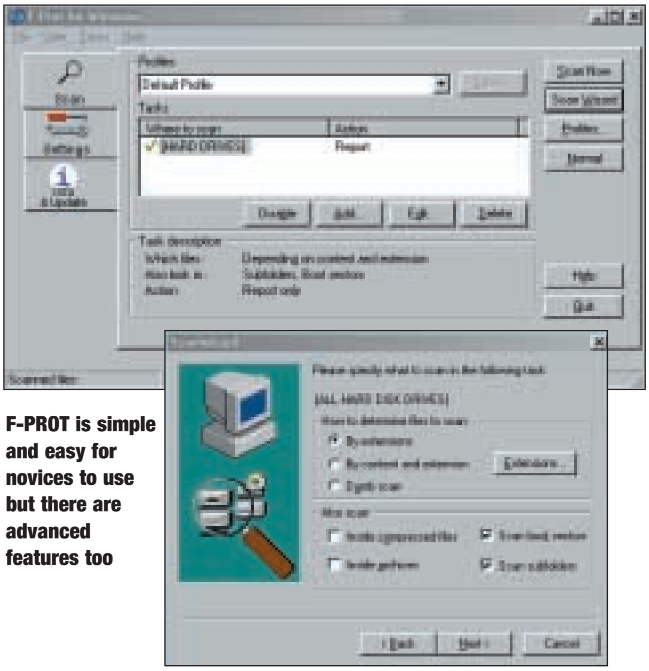
FP-WIN doesn't include any frills like scheduling or automatic updating, but it works well, new versions are continuously being released, it is easy to use and takes up few resources.

The modules, including the on-demand and the on-access scanner, can be configured individually, but it's easier to use the main graphical user interface. F-PROT for Windows is straightforward, but a Scan Wizard is added so you can skip through a series of point-and-click options to set up a manual scan.

A particularly good feature of Frisk Software's F-PROT is the ability to set up advanced tasks that perform very specific scans on certain files or folders. For example, you could create a task that scanned one set of folders with a quick scan and another task that scanned other folders more intensively. Groups of tasks are collected into a project, so that all the tasks run when the project is started.

F-PROT is easy for anyone to use, but its design makes it attractive to advanced users who'll appreciate the fine-grained control it brings to virus scanning.

Another module in the package, F-Check, maintains databases of objects such as folders and boot sectors, which are tracked for any changes that might suggest some suspicious activity. F-PROT is not the flashiest package around, but it has a well-considered feature set and is continuously updated.


Profile: Default Profile
Tasks:

Where to scan	Action
✓ [HARD DRIVES]	Report

Task description
Which files: Depending on content and extension
Also look in: Subfolders, Boot sectors
Action: Report only

Please specify what to scan in the following task:
[ALL HARD DISK DRIVES]
How to determine files to scan:
● By extensions
○ By content and extension
○ [illegible]
Also scan:
□ Inside compressed files ☑ Scan boot sectors
□ Inside archives ☑ Scan subfolders

F-PROT is simple and easy for novices to use but there are advanced features too

Kaspersky
AntiVirus Gold version 3.5

PCW Editor's Choice

PRICE £27.60 inc VAT **CONTACT** Kaspersky 01223 576 001 **www.kasperskylab.co.uk**

SYSTEM REQUIREMENTS Windows, 4MB of RAM, 9MB hard disk space

PROS Hard to beat; excellent service and support **CONS** Can be confusing for first-timers

OVERALL Great product that has a steep learning curve for absolute beginners

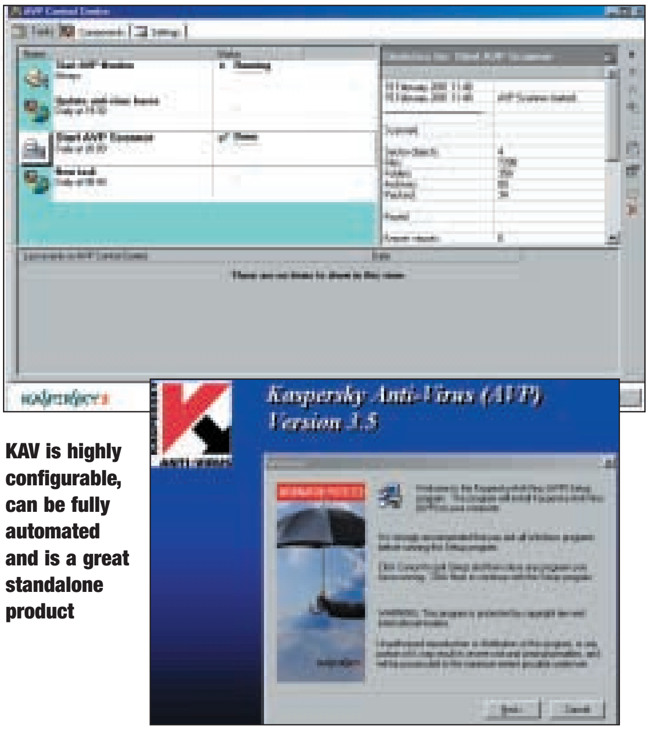
SCORE ■■■■■

The default install of Kaspersky AntiVirus (KAV) works so well you might never need to configure it again if the defaults, which include daily scheduled on-demand scans and automatic updates, are right for you. Its common name is AVP (Anti-Viral Toolkit Pro). However, the name is changing to Kaspersky Anti-Virus (KAV) because the owner of AVP.COM is now selling a product called AVX, causing some confusion among AVP users. So we're looking at KAV (formerly known as AVP) from kaspersky.com.

KAV consists of five main modules: the Monitor, Scanner, Updater, Script Checker and Control Centre. The script checker doesn't have a user interface. It's a separate heuristic engine that traps Windows scripts (wsh, vbs, Java, etc) arriving by email, before they're executed and passed to the Monitor for checking. The function is similar to POP3 email scanning but doesn't suffer from the configuration problems the POP3 method exposes. It works for any incoming script including those that run when surfing the web.

The Monitor provides the main on-access scanning engine and runs continuously in the background. The Scanner is for on-demand scanning, the Update for scheduling automatic updates and the Control Centre is for all the components and provides the scheduling and reporting functions. This can be confusing as the Scanner and Monitor can be opened at the same time as Control Centre and customised independently. That's the only real downside to KAV, which is hard to fault on performance or capability. It's highly configurable, can be fully automated, and is an excellent standalone anti-virus product.

In a networked environment, Control Centre provides the client access point for remote management, but on a standalone system KAV can be installed without the Control Centre (losing scheduling and reporting). KAV Gold, the version we tried, runs on Windows 95, 98, NT, 2000 and Me. A cut-down version called KAV Lite, which is easier to use, runs only on Windows 95 and 98. KAV Lite can be upgraded to KAV Gold for about £12.


AVP Control Centre
Kaspersky Anti-Virus (AVP)
Version 3.5
There are no items to show in this view.

KAV is highly configurable, can be fully automated and is a great standalone product

Network Associates
McAfee VirusScan 5.11

PRICE £27.03 inc VAT **CONTACT** Network Associates 0800 092 7160 **www.mcafee.com**

SYSTEM REQUIREMENTS Pentium, Windows, 32MB of RAM, 40MB hard disk space

PROS Efficient scanning with all the trimmings **CONS** Confusing to the newcomer

OVERALL Not bad, but could do with an interface overhaul

SCORE ■■■□□

McAfee VirusScan's colourful control panel is a surprise, but serves a useful purpose by gathering the main configuration elements of the various utilities into its appliance-like embrace. Regular operations like on-demand scanning, quarantining, and scheduling are easily accessed.

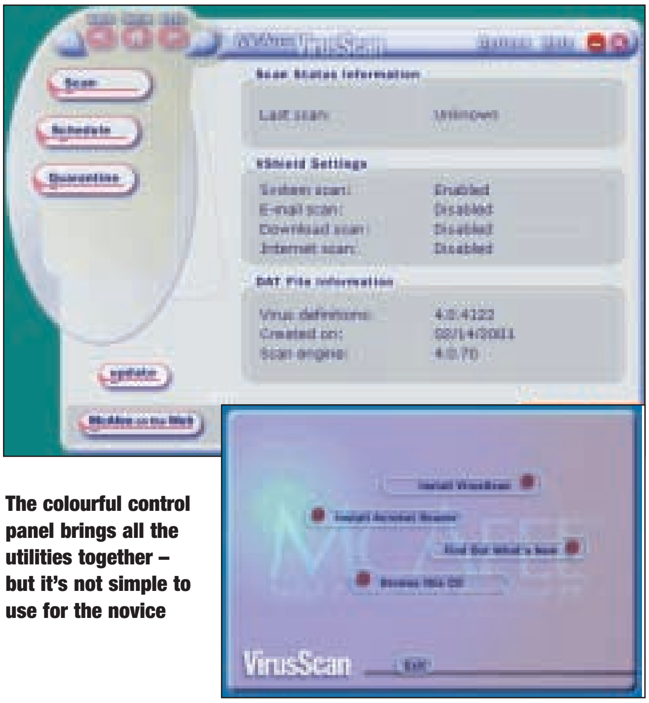
Beyond that, McAfee has lots to control and windows appearing all over the place can be confusing for some users. VShield Wizard, however, cuts through some clutter to configure the main background scanning options.

Although it's good to be able to tailor anti-virus software to your needs, having so many options can be intimidating, and a few more wizards wouldn't go amiss. Fortunately, once you've chosen your options you can preserve them with a password-protection feature. This also appears in the scheduler, so you can protect the scheduled tasks you've configured.

Scanning quality is good; McAfee was one of the few scanners to catch 'Kournakova' without an update. In speed terms it's slow, but doesn't impact on your work while the on-access scanner is whirring in the background. The on-access scanner normally looks for viruses it knows but can be configured to use a heuristic scan mode, which looks for suspected viral activity. This can be applied to documents, program files or both.

In addition to regular system scanning, McAfee has all the extra features that define the home-user anti-virus product and then some. VirusScan offers email scanning, Internet download scanning, and will scan for malicious objects on web pages. Once configured, these can be enabled and disabled individually from the Taskbar icon for the on-access VShield scanner that runs in the background.

McAfee VirusScan runs on Windows 95, 98, Me, NT4 (SP4) and 2000 desktops. This version doesn't support servers. VirusScan is a relatively full-featured scanner with all the trimmings, which adds up to 26MB sprawled over your hard disk. This isn't ideal and the multitude of configuration options is another weak spot. It's a little too anarchic for the user who wants to keep it simple and for everything to just work.



Scan Status Information

Last scan: Unknown

VShield Settings

System scan: Enabled
E-mail scan: Disabled
Download scan: Disabled
Internet scan: Disabled

DAT File information

Virus definitions: 4.0.4122
Created on: 02/14/2001
Scan engine: 4.0.70

The colourful control panel brings all the utilities together – but it's not simple to use for the novice

Norman Data Defense Virus Control version 5.00.18

PCW Editor's Choice

PRICE £47 inc VAT **CONTACT** Norman 01908 520 900 www.normanuk.com
SYSTEM REQUIREMENTS Windows, 16MB of RAM, 20MB hard disk space
PROS Excellent automatic update; near invisible in use **CONS** Absence of uninstall option
OVERALL All-round good performer and network-ready
SCORE ■■■■■

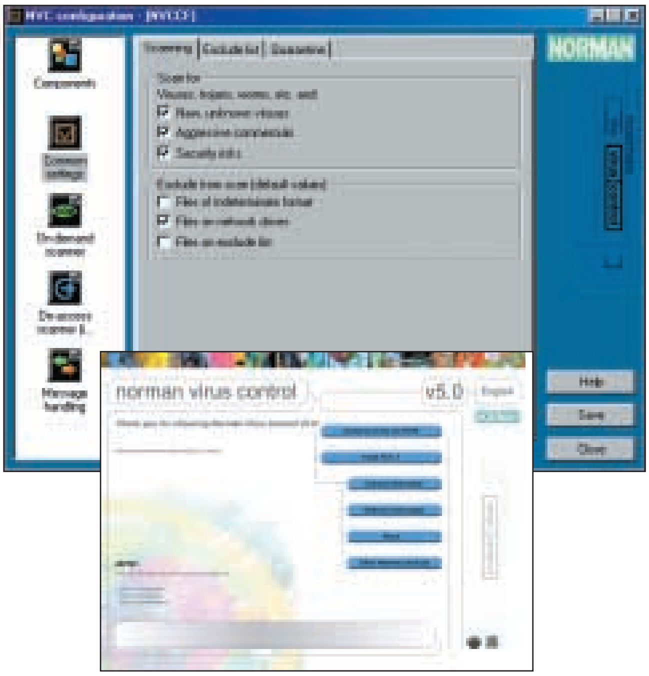
Norman Virus Control (NVC) tries hard to make installation easy and informative. When the CD is activated it autoruns a Flash-based graphical screen that leads into the install program that has links to useful information on the CD and on the web.

After installation completes the program shows a window suggesting you connect to the Internet and download the latest updates and upgrades. This is the Norman Internet Update system. It can be configured to connect automatically on a regular basis to stay up to date with software upgrades and virus signatures, which are continually updated rather than released on a time schedule.

A shortcut is installed by NVC on the right of the Windows Taskbar, which gives quick access to the program modules and a few preconfigured scanning tasks. You can also create specific tasks and set the scheduler to run them at specified intervals. NVC's scanning options are very flexible. The package can be configured to scan any selection of files, clean them if possible, move them to quarantine, or simply prompt for user action if a virus is detected. The user interface is generally clear and easy to use, but some of its on-access scanning options are a little obtuse and there is a possibility of setting it to do the opposite of what you intend.

NVC tries to make the scanning invisible, but standalone users might like some indication that something is happening. After automatically downloading the upgrade, for example, there was no indication that files were being upgraded, until a while later when a message appeared saying it had completed.

We ran on Windows 98 but NVC also supports 95, Me, NT and 2000. An OS/2 version is planned. NVC works well as a standalone scanner but is more oriented towards networked environments (NetWare or NT). The network orientation may explain the unusual absence of an uninstall option. To uninstall, a utility has to be downloaded from Norman.



You can configure NVC to scan a selection of files, clean or quarantine them, or just prompt for user action

Sophos Anti-Virus version 3.41

PRICE £116.91 inc VAT **CONTACT** Sophos 01235 559 933 www.sophos.com
SYSTEM REQUIREMENTS Pentium, Windows, 8MB of RAM, 4MB hard disk space
PROS Fast; easy to use; networked **CONS** Overkill for home users and small businesses
OVERALL Best left to the network administrators
SCORE ■■■□□

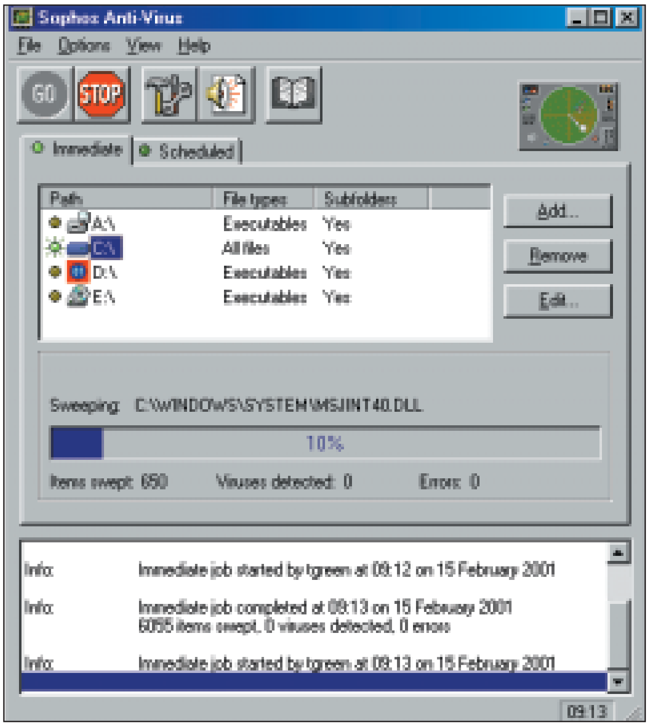
Sophos Anti-Virus provides on-access, on-demand scanning and disinfection, and works on most platforms. It doesn't really cater to the end user since it's aimed at corporate networks – tracking down the end-user price wasn't easy. Sophos prefers to sell network licences that allow Sophos Anti-Virus to be used on any mix of the platforms it supports. These include DOS; Windows 3x, 95, 98, NT, 2000 and Me; the Macintosh; and OS/2. Server versions support Unix, Windows, NetWare and OpenVMS networks.

Sophos Anti-Virus includes an agent component that enables a network administrator to configure, manage and update all Sophos clients from a single central location. The clients also send automatic alerts of virus activity on client systems to the central administrator. Licensing for small businesses starts at £395 ex VAT for a server plus up to nine clients, support and a year's worth of monthly software upgrades and virus signatures. Sophos makes additional updates available as and when necessary, and these can be downloaded automatically.

However, Anti-Virus works very well as a standalone version. It's quick to install and easy to configure. It runs unobtrusively in the background and has a barely noticeable effect on normal operations in its default scanning modes.

There are two modules, InterCheck and Sweep. InterCheck, the on-access module, runs in the background and monitors all files for potential virus activity. Sweep is the on-demand scanner that provides an intuitive configuration interface. Manual scans can be triggered at any time or can be preset to run at specific times or at intervals with the scheduler. The range of files to scan and the depth of scanning can be preset. Sweep will check all files including Zip archives or only those parts of files likely to contain viruses. As with many anti-virus scanners, InterCheck won't probe archived files unless asked to.

Sophos standalone is flexible enough to meet most needs and support is available via phone or 24-hour email, 365 days a year. Evaluation copies of the product are available but cannot be updated.



Path	File types	Subfolders
A:\	Executables	Yes
C:\	All files	Yes
D:\	Executables	Yes
E:\	Executables	Yes

Sweeping: C:\WINDOWS\SYSTEM\MSJINT40.DLL

10%

Items swept: 650 Viruses detected: 0 Errors: 0

```
Info:    Immediate job started by tgreen at 09:12 on 15 February 2001
Info:    Immediate job completed at 09:13 on 15 February 2001
         6055 items swept, 0 viruses detected, 0 errors
Info:    Immediate job started by tgreen at 09:13 on 15 February 2001
```

You can get Sweep, the on-demand scanner, to run at any time

Symantec Norton AntiVirus 2001

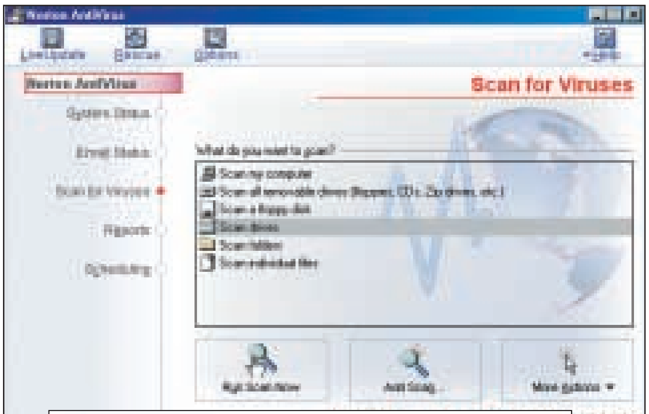
PRICE £29.99 inc VAT **CONTACT**: Symantec 020 7616 5600 www.symantec.com

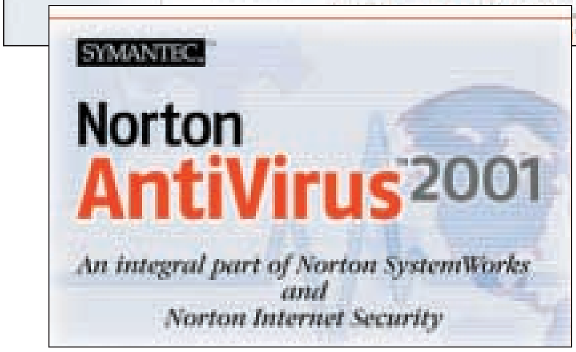
SYSTEM REQUIREMENTS Pentium, Windows, 32MB of RAM, 50MB hard disk space

PROS Almost transparent in use **CONS** Myriad options may prove confusing for beginners

OVERALL The Big Daddy of anti-virus software in every respect

SCORE ■■■□□





Norton is the big name in the anti-virus world and it's big on hard disks too. It installs 37MB of files, including 15MB into various folders in the Windows hierarchy. Installation is slick and it's good to see the recommendation to retrieve updates immediately after rebooting, as nothing dates faster than virus signature files.

Virus updates are collected by LiveUpdate, a feature common to all Norton utilities, which keeps the program software updated. After the initial update you can choose to have LiveUpdate prompt you before doing its stuff or allow it to work automatically. Automation is a high priority in Norton and most of it is set by default or through a few questions during install. Norton will scan and update automatically and will even detect an open Internet connection and make use of it to run LiveUpdate. The scanning options are comprehensive and there's only one interface into which other Norton utilities will integrate.

Norton AntiVirus has developed a reputation for being top heavy, so the company has been working on streamlining the scanning process. Norton's SmartScan engine reduces the performance hit when scanning by only searching for files with executable code and then scanning that code. It seems to work as Norton took only five seconds more to scan 12,000 files when told to scan all, than it did when it scanned program files and found 8,000. Its scanning speed is good, and overall performance impact reasonable.

Norton AntiVirus 2001 runs on Windows 95 (OSR2), 98, Me, 2000 and NT4 Workstation (SP4) and has much to commend it. The bootable CD for rescue is an excellent idea and its use of the Windows Scheduler instead of adding its own, cuts down on excess code but here's the rub. Norton takes up almost twice as much disk space as other products on the market. Disk space is cheap but that's not the point. The more one installs on Windows the higher the likelihood of glitches. Norton is feature-rich but in the anti-virus business, less is more.

Scanning speed is good and performance impact is reasonable

Trend Micro PC-cillin 2000/version 7.51

PCW Highly Commended

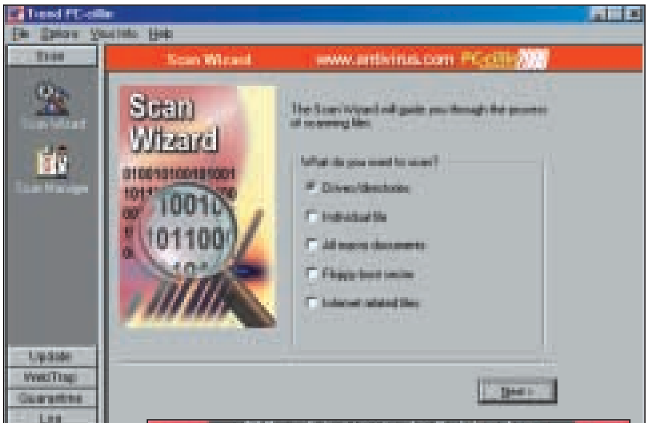
PRICE £29.50 inc VAT **CONTACT** Trend Micro 01628 400 500 www.trendmicro.co.uk

SYSTEM REQUIREMENTS Pentium, Windows, 24MB of RAM, 12MB of hard disk space

PROS Easier than falling off a log **CONS** Too easy for some

OVERALL Good stuff but should encourage users to learn more about security

SCORE ■■■■□



All the antivirus you need in the Internet age
PC-cillin 2000
AntiVirus
Install
User's Guide
Readme
Requirements
Exit
© Copyright 1988-2000 Trend Micro Incorporated

It's easy to see where PC-cillin 2000 (known as version 7.1 in the UK) is going as you run through the Install and see options for 'Parental Web Filtering' and 'Malicious Object Protection'. If you've used a more traditional anti-virus scanner this might seem odd – malicious object protection is what scanners should do; and what's web filtering doing there? PC-cillin leaves no doubt – you're entering home-user territory.

Malicious Object Protection is PC-cillin-speak for protection against unpleasant Java and ActiveX surprises you may come across via unscrupulous websites. It's not offering more than any good anti-virus scanner and some may think it's a little OTT, but in its defence it does alert the average home user to dangers they might not consider. Web filtering does what it says and allows parents some control over permitted websites. It sets a bar that also serves as a test of a child's ingenuity, but it's no substitute for concerned parental guidance.

PC-cillin offers POP3 email scanning for Outlook Express, and it scans Outlook folders, unlike some packages. These features, which aim to capture viruses in the incoming stream rather than once they've arrived, are aimed at Outlook because it's widely used by home users and frequently abused by email viruses. On the face of it, that's good, but it doesn't correct flaws in Windows, which makes Outlook inherently unsafe and could lead to a false sense of security. Also, POP3 scanning can be tricky to set up sometimes.

That aside, PC-cillin has lots to commend it as a home-user's choice. Its user interface follows the Outlook design guide, there's plenty of colour and graphics, it's easy to configure and works well. It supports Windows 95, 98, NT4 and 2000 but it's sold under different names in the US (PC-cillin 2000) and in the UK (PC-cillin version 7). If you download a trial version or buy it online (at $29.95) it'll be PC-cillin 2000 because the website is in the US, but the version number (7.xx) will be displayed in the program's Help/About box.

For the home user this is easy to use, with its interface following Outlook's design, and it's easy to configure

HOW WE TEST

Without access to viruses 'in the wild' we can't perform credible real-world tests – but other labs can

We have not lab tested these anti-virus software packages ourselves because the only centres that now perform credible 'real world' tests, are either academic institutes or levy a charge for testing. Over 50,000 viruses exist 'in the wild' outside the confines of a virus research laboratory or an individual's sole possession. Unless we test each product against every virus known to be in circulation we cannot say that we have performed a valid test. Picking a representative sample, no matter how large, says nothing about the efficiency of the anti-virus product and much about our ability to source viruses.

Another reason for not doing the test ourselves is that all the viruses now in circulation have got there either because they were deliberately released into circulation, or because they 'escaped' accidentally. With the best will in the world, viruses do escape. Accordingly, the vast majority of the anti-virus research community has adopted a strict policy against exchanging viruses with anyone other than those whom they implicitly trust – and that trust circle is small.

We do not feel a magazine conducting a limited group test qualifies for inclusion in the group that has access to the 'wild list', and there is no good reason for increasing the risk of spreading viruses in order to test a subset of the anti-virus product range when several exhaustive independent tests are available.

For objective assessments of anti-virus products we viewed the results of the Virus Test Centre (VTC) at the University of Hamburg (http://agn-www.informatik.uni-hamburg.de/vtc/naveng.htm), and West Coast Labs (www.check-mark.com/) an independent UK-based test centre. Both perform detection and cleaning tests based on the entire 'wild list'. The VTC is an academic institution while West Coast Labs charges a fee for Check-Mark certification. Our group test takes a subset of the full range of anti-virus products, focuses on Windows 98, and uses the latest version at the time of writing. Since lab tests take time, some recent product versions had not been tested at the time of writing, but past results serve to establish a product's track record.

Our Editor's Choices are based on subjective tests: suitability to task, ease of use, track record, and the quality of support on offer. We've also used atypical scenarios – copying large numbers of files with on-access scanning set to check every file; simultaneously opening multiple large documents while running on-demand scans of all files – to gauge performance impact.

The Virus Test Centre and West Coast Labs carry out objective tests on viruses in the wild

AVOID THE RISK OF INFECTION

Nowadays we're all more connected and this provides fertile ground for the authors of malicious software often called 'malware', that can damage your data and which may spread from your computer to others. This can happen over the Internet and company networks or via data exchange, for example through a floppy disk or a CD. Malware spreads in many ways including file exchange and malicious HTML but most of the attacks that spread 'in the wild' rely on scripts (Microsoft VBS and Word macros) and spread via email.

Malware may prevent you from using your computer and in extreme incidents can render media such as hard disks unusable. In such cases only a backup can save your data. Backup strategies should account for the possibility of malware damage not being detected immediately. A good strategy is to cycle through at least three backup sets over time and to archive (set aside) one on a regular basis.

Malware is most prevalent on Windows as that's what most people use and it's an easy target. But it can also attack Apple Macs, Unix (including Linux), and machines running Java. Malware attacks on handheld devices, such as the Palm and mobile phones, have not been successful yet. But as such devices become more prevalent and increasingly interconnected the risks become higher.

Anti-virus researchers define specific categories of malware – viruses, worms, trojans, backdoors, hoaxes, and jokes. But there's invariably some fuzziness in the specifics, not least in the following abbreviated definitions!

A 'virus' is self-replicating (can infect another file) and may contain a payload (for example, it may damage data or display a message).

'Worms' copy themselves to other computers by means of networks, very often using email, and may carry a payload such as a virus.

'Trojans' are non-replicating programs which carry a payload that has an unintended effect. This may be benign (a joke for instance) but it could install malware on your system, for example a 'backdoor' that alerts people when you're online and allows them to access your computer data or use your computer to attack others.

'Hoaxes' try to get you to perform some act, which may be trivial or damaging. 'Jokes' may appear to be harmless and often are, but they have been used to deliver malware and should be avoided, no matter how amusing, purely because they encourage people to be complacent about opening unknown attachments.

Windows machines suffer most from malware, but others, such as Apple Macs, are also vulnerable, so be aware of the risks and avoid those nasty bugs

TABLE OF FEATURES

MANUFACTURER	COMMAND	COMPUTER ASSOCIATES	F-SECURE	FRISK SOFTWARE	KASPERSKY LABS
PRODUCT	ANTI-VIRUS	INOCULATEIT PERSONAL EDITION	F-SECURE ANTI-VIRUS	F-PROT FOR WINDOWS	KASPERSKY ANTI-VIRUS GOLD
Version	4.60	5.2.5	5.21	3.08c	3.5
Telephone	020 7931 9301	Web only	01223 478 800	+354 561 7273	01223 576 001
URL	www.command.co.uk	http://antivirus.cai.com	www.F-Secure.com	www.complex.is	www.kaspersky.com
Price inc VAT	£58.69	Free	£84.60	N/A – online	£27.60
Price ex VAT	£49.95	Free	£72	$25 (£17)	£23.49
Includes support	12 months	Lifetime	12 months	12 months	12 months
Trial copy	30 days	N/A	Not yet available	30 days	Unlimited; no updates
Windows platforms	3.1/95/98/NT/2000	95/98/Me/NT/2000	95/98/NT/2000	95/98/NT/2000	95/98/NT/2000
Other operating systems	DOS, NetWare, OS/2, Linux	✗	✗	✗	DOS, Linux
Network ready	✓	✗	✓	✗	✓
Auto update	Network	Internet	On demand	✗	Internet
Support advisories	Online	email	Online	Online	email
On-demand scanning	✓	✓	✓	✓	✓
On-access scanning	✓	✓	✓	✓	✓
Auto document clean	✓	✓	✓	✓	✓
Auto file clean	✓	✓	✓	✓	✓
Quarantine feature	✗	✗	✗	✓	✓
Intelligent/heuristic scanning	✓	✓	✓	✓	✓
Scheduler	✓	✗	✗	✗	✓
Customised tasks	✓	✗	✗	✓	✓
POP3 email scanner	✗	✗	✗	✗	✗
Web filtering	✗	✗	✗	✗	✗
Hard disk space required	9MB	4MB	25MB	4MB	9MB

MANUFACTURER	NETWORK ASSOCIATES	NORMAN DATA DEFENSE SYSTEMS	SOPHOS	SYMANTEC	TREND MICRO
PRODUCT	MCAFEE VIRUSSCAN	NORMAN VIRUS CONTROL	SOPHOS ANTI-VIRUS	NORTON ANTIVIRUS 2001	PC-CILLIN 2000/ VERSION 7.51
Version	5.11	5.00.18	3.41	2001	7.51.0.1060
Telephone	0800 092 7160	01908 520 900	01235 559 933	020 7616 5600	01628 400 500
URL	www.mcafee.com	www.normanuk.com	www.sophos.com	www.symantec.com	www.trendmicro.co.uk
Price inc VAT	£27.03	£47	£116.91	£29.99	£29.50
Price ex VAT	£23	£40	£99.50	£25.52	£25.11
Includes support	12 months	12 months	12 months	12 months	12 months
Trial copy	30 days	30 days	30 days	30 days	30 days
Windows platforms	95/98/Me/NT/2000	95/98/Me/NT/2000	3.1/95/98/Me/NT/2000	95/98/Me/NT/2000	95/98/Me/NT/2000
Other operating systems	Mac	OS/2	Mac, Unix, DOS, OS/2	Mac	✗
Network ready	✓	✓	✓	✗	✗
Auto update	Internet	Internet	Network	Internet	Internet
Support advisories	Online	Online	Online	Online	email
On-demand scanning	✓	✓	✓	✓	✓
On-access scanning	✓	✓	✓	✓	✓
Auto document clean	✓	✓	✓	✓	✓
Auto file clean	✓	✓	✓	✓	✓
Quarantine feature	✓	✓	✓	✓	✓
Intelligent/heuristic scanning	✓	✓	✓	✓	✓
Scheduler	✓	✓	✓	Windows	✓
Customised tasks	✓	✓	✓	✓	✓
POP3 email scanner	✓	✗	✗	✓	✓
Web filtering	✓	✗	✗	✗	✓
Hard disk space required	40MB	20MB	4MB	50MB	12MB

Anti Virus!

Editor's Choice

Anti-virus scanners have a tough job – to stop malicious software perturbing us and doing so almost invisibly. Scanners must operate in the background and catch viruses while remaining almost invisible, because nothing is more likely to result in a scanner being disabled or removed than a perceptible effect on performance or an over-zealous presence. When a new virus spreads rapidly, scanners are expected to trap them even if the virus didn't exist at the time the scanner was installed. Sometimes they fail but, surprisingly, the top scanners succeed more often than not, because they have become very good at detection and at cleaning up after an infection.

But there are two things scanners cannot do: change human nature and fix problems inherent in the operating system or apps we use. To reduce the risk from malicious software, in addition to using a scanner, avoid opening unexpected attachments and don't send unnecessary attachments.

We have picked Editor's Choices in two task categories: home user is distinguished by simplicity in standalone use; the small-business category takes network adaptability into account. We've chosen one runner-up but could have picked more as the quality of scanners has improved markedly over the years, even as the job has become infinitely more difficult. Winners have also been selected on the basis of frequency and ease of updates, the degree to which they adapt to typical working habits, the quality of support and track record.

No scanner is perfect in every respect but some have a better track record than others. Not so long ago it was rare to upgrade virus definitions, the files that detect specific viruses, more than a few times in a year unless there was a big threat that called for an emergency update. As the frequency with which new threats arrived increased, so did the update frequency. In the past year many scanner vendors have started shipping daily updates.

Anti-virus scanners need to be very flexible but this should not be at the expense of ease of use. They also need to offer a high degree of automation in order to operate in the background without giving the user any reason to disable them. For the same reason they shouldn't make too many demands on the system while still working hard to discover viruses wherever they are and however hard they try to hide. On top of this scanners need to offer top-notch support when a virus is detected or suspected, as this is invariably a very stressful time. Our Editor's Choices meet these demands.

The winners

The **Editor's Choice** for a home-user package goes to **Kaspersky Anti-Virus Gold 3.5**. While not the simplest package, it does the most with the least amount of fluff. A default install meets the needs of most users but offers the fine-grained control more experienced users can tune to their exact needs. Automatic updates can be scheduled daily because the signature bases are updated daily (or more frequently as required). When we emailed an urgent out-of-hours request for support it wasn't only answered satisfactorily, it was answered quickly, in under an hour.

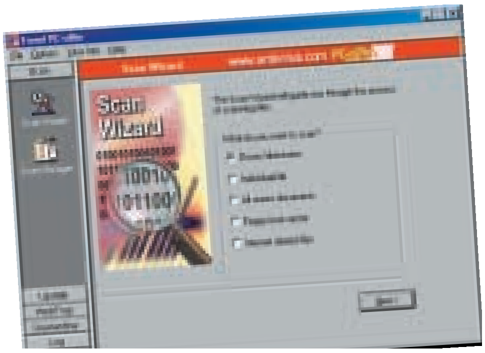
The **Editor's Choice** for a small business package with network connectivity goes to **Norman Virus Control 5.00**. It can be installed and virtually forgotten, appearing only when needed. It also has the right level of control for more advanced configuration; offering automated updating over the net and continuous releases of signature updates. The program itself is regularly updated. An out-of-hours, emailed support request was answered within a couple of hours. In addition, although it's well suited to standalone use, Norman Virus Control is specifically designed for use on a network.

Our **Highly Commended** gong goes to **Trend Micro's PC-cillin**. Although we have some reservations about the feature set, there's no doubt PC-cillin is a workable all-round package for home users and individual PCs in small businesses with no need for network services. Almost everything is automated including virus signature updates; the user interface is relatively restrained; and, although it chews up around 20MB of hard disk space, that only puts it in the midrange of this pack. It also has most of the 'must-have' features of the big boys – quarantine for suspected infections, heuristic scanning for unknown and new viruses, custom scheduling, and support for Windows 2000 and Me.

Scanners need to be flexible but not at the expense of ease of use

Kaspersky
AntiVirus Gold version 3.5

Norman
Virus Control version 5.00.18



Trend Micro
PC-cillin 2000/7.51