

Find the right package to help you stay safe online. **Richard Cobbett** shows you what to look for, and rates ten of the best AV to help you deal with anything that gets in your way

Depressingly, antivirus software has never been more important. In the old days, you could – just about – get away with not bothering, simply by making sure you didn't run any dodgy software, stayed clear of some obvious online traps, and kept backups of all your important files. A virus might sneak through and nuke your system, but if you'd made plans, you knew you were covered.

No longer. Modern viruses are a very different beast. They don't for the most part care about deleting your files, or even making their presence known. Instead, they try to infest your PC, turning it into part of a botnet that anyone with a little bit of money and a grudge can use to launch illegal attacks on any target in the world. They hide in the background, waiting to swipe your credit card information and social network logins or even (gasp) your *World of Warcraft* account. A modern virus could be a thief, a terrorist tool, a child porn downloader

or anything else, and if it gets you in trouble, good luck persuading the authorities of the fact. Far better to be safe than sorry.

But which antivirus tool to get? Just because you need one doesn't mean you have to pay for it, and the fact that some have more features than others can quickly become a problem if they turn out to be so intrusive or system-intensive that you end up simply shutting them off.

Luckily, we're on your side. We've pulled together the biggest and best tools and run them through their paces, as virus scanners and apps in their own right. We've rated them on their scanning performance, their system requirements, their update cycles and more, and over the next few pages, we'll show you exactly what to look for in your new watchdog. Some are better suited for gaming, others pack in lots of extra features that you may find handy. Some offer free versions or alternative versions that don't pack in standard extras such as firewalls. All of them are ready and willing to keep you safe. You need one of them. The only question is which one is right for you.

The firewall trap

It burns, burns, burns...

The main difference between 'antivirus' and 'internet security' editions of most antivirus products is the addition of a firewall. You might think that you're already safely covered here, since Windows comes with one built-in, but in practice it's a very weak one. By default, it doesn't give you much control. If you dig a little deeper, you get mired in the horrors of policy management. It's better than nothing, but not by a huge amount, especially given how many alternatives there are.

A firewall's job is to monitor internet communications, preventing anything that shouldn't from getting in, and just as importantly, anything that shouldn't be allowed to get out from leaking. Spyware for instance is no use to its creator if it can't actually send them your stolen information.

There are two kinds of firewall you can make use of: software and hardware. Chances are you already have a hardware firewall close to

hand, built into your broadband router. Firewalls can be complicated to set up, being based around opening and closing specific ports on your network, preventing any traffic from escaping without your express permission.

Software firewalls, such as the one in Windows, work on a different level, approving or denying individual pieces of software as and when necessary. This makes them much easier to configure, but your rules only apply to that computer. If someone brings in an infested laptop for instance, it could still abuse your network.

Because of this, even if you do have a software firewall in place, it's worth taking the time to lock things down a bit more. Check your router's manual to find where it keeps those settings. (Typically, this is in an Advanced Security panel in its browser-based configuration screen). You can also try checking on the internet to see which ports to open up and lock down for services, such as online games and BitTorrent.

Getting a firewall running properly can be a time-consuming and fiddly task, but one that you hopefully only have to do once (at least until re-installing Windows or buying a new router). Without one in place, your antivirus may be a good guard-dog, but it's still patrolling a castle with no moat.

Initial performance

The impact of antivirus on boot-up

Whichever antivirus suite you install, there will be an immediate knock to your system's performance, starting with boot-up.

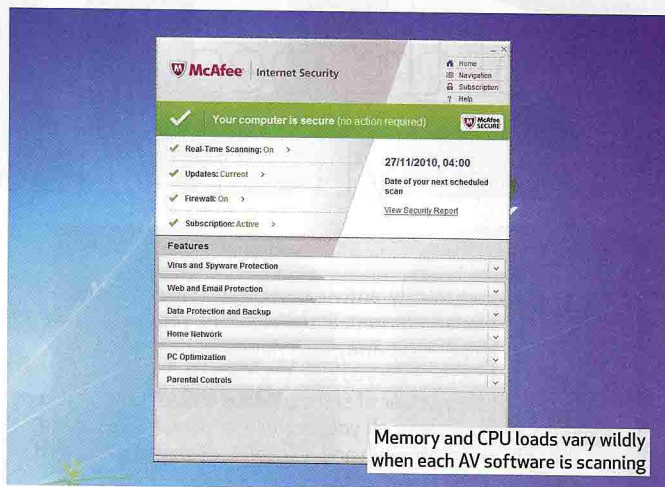
On our test system, a standard boot took precisely 38 seconds from initial switch-on to Windows being ready to go. The best bootup performer here: Trend Micro Titanium Internet Security 2011 added a mere six seconds onto this. Most of the antivirus software floated around the additional 30 second mark. The worst, PC Tools Internet Security 2011, added a full minute and fifteen seconds.

It's worth noting that your performance here can usually be improved by not using firewall components, although that's not recommended unless you already have a firewall running on your

router, and that you can still get started on using your PC once Windows has booted, even if some software has yet to fully finish loading. The best performers in this particular test floated around the 15 second mark, which will be barely noticeable if you're not specifically timing it. Beyond that, it can be an irritation.

RESULTS (SECONDS)

AVG IS 2011	55
BitDefender IS 2011	71
Kaspersky Pure	72
McAfee IS 2011	73
Microsoft Security Essentials	48
Norton IS 2011	56
PC Tools IS 2011	113
Trend IS 2011	44
VIPRE AVP	71
Webroot IS	59



Memory/CPU load

The cost of having AV on your system

Every program here takes up valuable system resources whether scanning your system or not. Even when not doing a full scan, they offer real-time checking of any files you download or access, just in case. Actually scanning your whole drive, which they do on a regular basis, is a very system-intensive process.

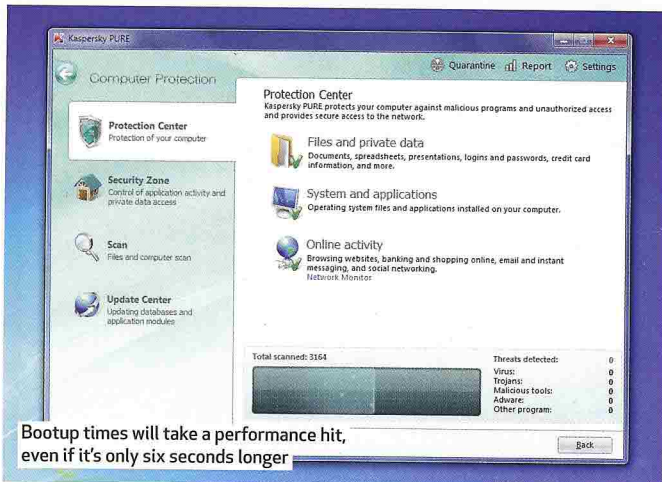
We tested the memory and CPU loads during scans to see which has the least impact. Bear in mind though that while these numbers are typically high, there are ways around them - notably scheduling full scans when you're not using your computer, or switching your antivirus software into a dedicated Gaming Mode (if the package supports it).

Memory usage turned out to cover the whole chart, with Norton

and McAfee among the best performers, and Trend and VIPRE in dead-last. In terms of CPU usage, Webroot and Norton* came out firmly in front. Microsoft's Security Essentials put in one of the most standard scores, with a mid-level performance in both areas - not bad for both a Microsoft product and a freebie.

RESULTS (LOAD)

AVG IS 2011	73.3%
BitDefender IS 2011	77.9%
Kaspersky Pure	73.9%
McAfee IS 2011	89.1%
Microsoft Security Essentials	67.2%
Norton IS 2011	15.2%
PC Tools IS 2011	44.5%
Trend IS 2011	67.5%
VIPRE AVP	73.1%
Webroot IS	32.9%



Scanning

The big one – how well did each package do at tracking down viruses?

When we talk about viruses (and it is viruses, not 'virii'), we're actually talking about a whole range of different types of attack, usually referred to as 'malware'.

A virus is a piece of malware that tries to spread itself, for instance by jumping into your email account and mailing itself to all your friends. Trojan horses are malware pretending to be something else, like a game, a porn site or – irritatingly – an antivirus program. Root kits are malware that bury down deep like a tapeworm, where they can affect Windows, but Windows can't even see them, never mind delete them. The list goes on, and a good antivirus program has to be able to catch all of them.

Most tools use two basic techniques: signatures and heuristics. Signatures involve running any programs or files that need checking past a master list, which is typically saved on your PC – but increasingly is being stored on the cloud – and simply recognising them.

Heuristics watch for what a program is trying to do, and step in if it looks dodgy. When an antivirus program detects a virus, we call that a 'true positive'. When it gets it wrong, it's either a 'false positive' if the program was actually safe, or a 'false negative' if it was actually a virus. The first is an irritating, but fixable issue – instead of simply deleting files, all antivirus programs quarantine them and let you restore them. The second is potentially disastrous, and most likely with

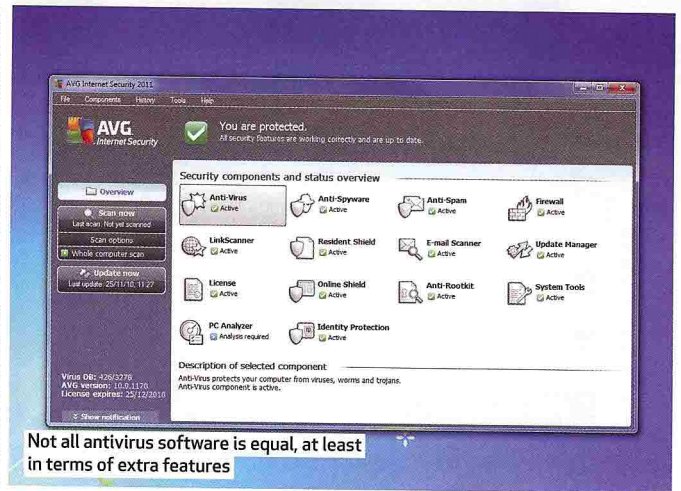
brand new malware that hasn't done the rounds yet.

The good news is that almost all of the products in this test shone, walking away with a perfect score. Our test involved putting each one up against a range of different nasty invaders, and sprinkling in a few false positives for good measure, and most earned 100 per cent at both.

However, there were exceptions. Webroot Internet Security slipped up, but still managed to deal with a creditable 97 per cent of the viruses. Trend Micro Titanium Internet Security only managed 76.5 per cent, though. That's definitely a weak performance, although it's worth bearing in mind that every antivirus tool has the occasional blind-spot over its run.

You might think that the fix is to run more than one at the same time, but unfortunately that's not a good idea. Doing that will simply cause them to clash and squabble, not to mention soak up most of your system resources for no real benefit. Like marriage, you have to pick and hope it works out.

RESULTS (SCAN TIME)	
AVG IS 2011	10.38
BitDefender IS 2011	16.48
Kaspersky Pure	16.03
McAfee IS 2011	17.33
Microsoft Security Essentials	25.25
Norton IS 2011	40.51
PC Tools IS 2011	33.40
Trend IS 2011	11.23
VIPRE AVP	12.38
Webroot IS	24.03



Not all antivirus software is equal, at least in terms of extra features

Bonus features

Highlighting a few of the handy extras that might change your mind

As a general rule, antivirus software tends to come in three forms: Antivirus, which does exactly that goes after viruses; Internet Security, which bolts on a better firewall than the standard Windows one; and typically a third version, with some extra toys to play with.

The exact load-out changes from product to product though, so it's worth checking the inevitable 'Compare Editions' tool on your chosen company's website to see what you'll actually need before deciding whether to splash out or save your cash.

Parental Controls are one of the most popular Internet Security additions, as demonstrated by both Norton and McAfee. These let you track what your kids are up to, and block access to dodgy sites. Other common additions include file shredders for safely deleting files, website filtering (typically via a toolbar, and thus reliant on you using Internet Explorer or Firefox rather than a browser such as Opera or Chrome), and a spam-busting module, although these are increasingly useless as more of us move to webmail systems, instead of relying on POP3 accounts in client applications such as Outlook and Thunderbird.

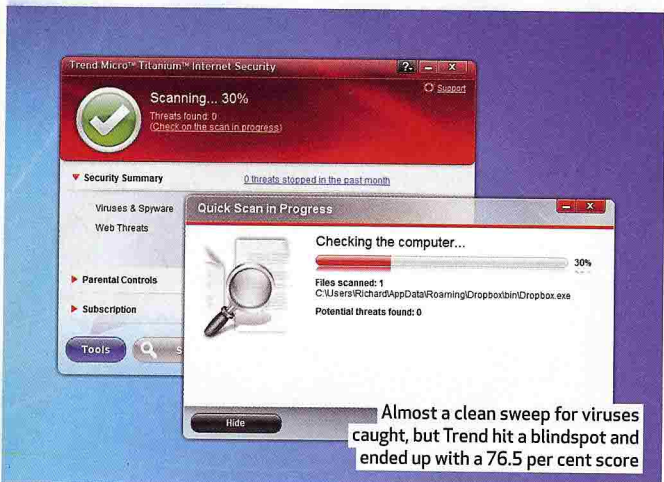
By far the most interesting extra in this year's batch of tools is Kaspersky Pure and its Safe Run feature. Most antivirus programs use 'sandboxing' technology to isolate a suspicious file. What this does is watch how a file acts when it thinks it has access to the system, and then decides how to

deal with the file, according to what it does.

Kaspersky opens this up to any of your applications, with the most useful being your web browser. Fire it up in Safe Run mode and the window is surrounded by a green radioactive glow, and appears to have full access to the system. Try to save a file to the Desktop however and it won't appear. To pass files out of this impromptu Matrix-like effect, when you're entirely sure that they're safe, Kaspersky supplies a shared folder.

For obvious reasons, we don't recommend using this mode to try out programs that you know are dodgy (if you must do that, create a dedicated virtual machine in a tool, such as Virtual PC, while remembering to shut off its access to the internet and preventing it from having access to any of your files at all), but it's a great addition, and a fun one to play with. It's worth noting though that while we reviewed the Pure version here, Kaspersky Internet Security 2011 also contains a version of this tool.

RESULTS	
AVG IS 2011	82%
BitDefender IS 2011	80%
Kaspersky Pure	90%
McAfee IS 2011	88%
Microsoft Security Essentials	60%
Norton IS 2011	89%
PC Tools IS 2011	81%
Trend IS 2011	79%
VIPRE AVP	80%
Webroot IS	77%



Almost a clean sweep for viruses caught, but Trend hit a blindspot and ended up with a 76.5 per cent score

