COMPARATIVE REVIEW

WINDOWS 2000 PROFESSIONAL

John Hawes

Windows 2000 is getting a little long in the tooth, having been superseded within two years of its release by *Windows XP* – whose slightly shinier surfaces seemed so revolutionary back in 2001 – and this year by the even shinier *Vista*. Despite its age and rather drab looks, Win2k soldiers gamely on, serving its purpose perfectly adequately for plenty of users and still being the operating system of choice in many homes and businesses.

For the developers of security products this represents something of a challenge. New platform versions will inevitably present plenty of new hurdles, with tweaks needed to various parts of the products, not least the interfaces to keep pace with the ever-improving look and feel of computer desktops. But while all this newness is being added there is also a duty for developers to keep in touch with the old.

While many (but by no means all) security vendors, including *Microsoft* itself, have retired support for the Win9x family, *Windows 2000* (currently held in an 'extended support' period by *Microsoft*) remains too big a market to drop, and its close proximity to current market leader *Windows XP* has meant that, in most cases, little extra work is needed to ensure mutual compatibility. Of course, with most development and QA eyes firmly on the more common, more recent platforms, bugs and troubles on older versions are more likely.

However, with yet another bumper crop of products to slog through in a somewhat short month, I hoped that the products would prove as stable, reliable and trouble free as the platform itself.

PLATFORM AND TEST SETS

Windows 2000 has been sitting on Service Pack 4 for several years, and as usual with VB100 tests the platform was used in a fairly bare state with no further updates added unless required by a specific product.

The installation and setup of *Windows 2000* was thus a fairly straightforward task, familiar from countless previous ventures down the same path, and complicated only by a lack of support for some components in the fairly new machines preferred for VB100 testing. Rather than face several weeks testing at low resolution, extra drivers were added to fully enable the modern graphics cards, as well as network interfaces, but otherwise the systems were left untouched. I expected some products to require updates, such as upgrading *Internet Explorer* or *Windows Installer* to more recent versions, but these changes were not made by default in order to ensure that products with such requirements could easily be identified.

The test sets were based on the most recent WildList available on 26 October, with the product submission deadline a few days later. This month, a spurt of hard work from the *WildList Organization* meant that the September WildList was available in plenty of time to be included, and it was upon this list that the main test set was based.

With a large number of new additions by recent standards, replicating and validating samples for the set was a bigger job than usual, but helped by the preponderance of familiar old names: large numbers of W32/Rbot and W32/Sdbot, with plenty of W32/Agobot and W32/Rontokbro and other similar items. There were a few less common additions, including plenty of file infectors, mainly from the W32/Looked and W32/Fujacks families, but including a W32/Virut variant which promised to present significant challenges in detection.

Also of note was the fact that, for the first time in a while, there was not a single new W32/Mytob variant to be added – a sign, perhaps, that this family is finally showing its age.

With a lot of lab time taken up with additions to the core set, expansion of the other test sets was limited. A sprinkling of items were added to the collection of worms and bots (mostly yet more variants of the major families) and the existing polymorphic test sets were expanded.

The clean set was enlarged with the usual selection of items, mostly from popular and recently released software packages on common download sites.

To assist in the presentation of speed results a small new set of files was added. With products offering some wildly different sets of default settings, the archive test has long presented problems when showing speed measurements, with products that do not scan inside archives unfairly showing better speeds than their more thorough rivals. To guide readers in interpreting these results, a set of common archive types has been created at various depths of nesting, with the Eicar test file at the bottom of each. A plain, uncompressed copy of the test file was added to check that it was indeed included in the detection, and as an extra, another copy renamed to a random extension was added to test scanning of non-standard filenames.

I created a rather arbitrary cut-off point, deciding that products should detect at least five levels deep in at least four of the eight archive types included in the set in order to be included in the 'all files' speed graphs, and below this level a product's scan times would only be included on the 'default settings' display.

AEC Trustport Antivirus 2.8.0.1607

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	99.94%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	15

Czech Republic-based *AEC* has been doing pretty well with its *Trustport* product, achieving some impressive scores in numerous tests thanks to its multi-engine approach. The product submitted here, the anti-virus component, is not available as a standalone product but is part of the *Trustport Workstation* suite, along with a swathe of other security solutions, and is rolled into a range of server and gateway products.

Installation of the product hit an immediate, if not unexpected stumbling block in the form of the requirement for *Internet Explorer 6* or newer. While this is not an extravagant demand, it does raise a small concern – it's more than possible that a user, having restored a system to an old safe state (perhaps using a rescue CD provided by the system retailer), would be in the position of running a bare *Windows 2000* installation, and would thus have to spend quite some time online in an entirely unprotected state to acquire the required updates. Given the scare stories that estimate the average infection time for an unprotected system connected to the web to be as little as ten minutes, this window of exposure could be unacceptable.

Once installed, *Trustport* presents a solid and reliable appearance with its graphics depicting well shielded footsoldiers – an image backed up by the multi-engine scanner at its heart. The product's makeup has changed somewhat since its last appearance, with the *BitDefender* engine included in earlier versions replaced by those of *Dr.Web* and *VirusBlokAda* – an interesting selection, not least as it includes an engine which has yet to appear on the *VB* test bench. A lot of heuristic technology hinted at a high risk of false positives, but could be expected to ensure pretty thorough coverage of infected items.

Tests were carried out easily, with the speed tests particularly straightforward as the default action is to scan all files, including the contents of archives, both on demand and on access. The new set of archive types was detected in depth, although neither of the engines implemented on access seemed capable of penetrating .LZH files – the on-access mode uses only two of the available scanning engines, though more can be added by the more paranoid user as long as they have the available processing power. Of course, multiple engines are unlikely to achieve the best speeds or lowest overheads, and speed figures here showed a pretty hefty drain on resources.

The many engines spotted a fairly large number of potentially unwanted items in the clean sets, a large number of which were system tools from *Sysinternals*, and all of which were labelled in the log with the rather stark and worrying 'Infected!'. However, their full definitions described them more accurately as tools or programs. As feared a few full false positives were also flagged, spoiling the product's chances of winning another VB100 award. More surprisingly, a few samples of the new W32/Virut variant were missed on access, indicating that these were likely to prove a problem for at least a few more products as testing continued.

Agnitum Outpost Security Suite Pro 6.0.2165.8226

ItW	100.00%	**Worms & bots**	99.74%
ItW (o/a)	100.00%	**DOS**	99.58%
File infector	98.86%	**Macro**	100.00%
Polymorphic	84.18%	**False positives**	0

Agnitum's product is fairly recent and almost certainly developed since the arrival of *Windows XP*. It showed no signs of requiring any extra software – at least until halfway through the installation, when an error message revealed the absence of a required DLL. This did not seem to be a fatal problem, and the installation continued to the requested reboot, on return from which the system froze in an unresponsive state.

Reimaging and trying the installation again with the extra DLL in place led to a much more complex installation process, with a series of configuration pages to be worked through before reaching the reboot phase. Again, the system failed to return – even safe mode seemingly inaccessible – and the developers were called for assistance. Investigation indicated that the problem related to the rather modern systems being used for the test, and when the test image was ported to more humble hardware there were no such difficulties.

With no clear way of circumventing the problems on the main systems, tests proceeded minus the speed test, which would have been all but meaningless on the considerably slower hardware.

The product looked good and proved pleasant to work with, offering a wide range of modules which sadly went unexplored. With good detection across the test sets and no false positives generated in the clean sets, *Agnitum* earns a VB100 award.

On-demand tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
AEC Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	15	19
Agnitum Outpost	0	100.00%	3	99.74%	28	99.58%	8	98.86%	0	100.00%	220	84.18%		
Alwil avast!	0	100.00%	7	99.69%	757	97.74%	0	100.00%	18	99.56%	657	85.69%	1	
Avira AntiVir	0	100.00%	0	100.00%	32	99.79%	0	100.00%	0	100.00%	3	99.85%	2	
BitDefender AntiVirus	0	100.00%	1	99.84%	8	99.79%	2	98.48%	1	99.98%	0	100.00%		
Bullguard Bullguard	0	100.00%	1	99.84%	8	99.79%	2	98.48%	1	99.98%	0	100.00%		1
CA Antivirus	20	99.18%	0	100.00%	235	99.70%	1	99.77%	0	100.00%	9	99.60%		
CA eTrust	0	100.00%	0	100.00%	235	99.70%	3	99.02%	12	99.82%	9	99.60%		
Doctor Web Dr. Web	11	98.50%	1	99.84%	0	100.00%	2	99.24%	0	100.00%	0	100.00%	2	2
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%		
Fortinet Forticlient	2	99.98%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	99.90%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%	1	
F-Secure Anti-Virus 2008	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		2
GDATA Anti-virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		4
Grisoft AVG	0	100.00%	5	99.86%	200	98.96%	7	97.73%	0	100.00%	695	76.07%		
Ikarus Virus Utilities	9	99.88%	6	99.81%	2461	91.37%	23	93.37%	171	96.07%	353	80.58%	13	31
Iolo Antivirus	32	99.71%	1	99.84%	0	100.00%	0	100.00%	0	100.00%	4	99.83%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		
Kingsoft AntiVirus	60	95.63%	600	18.23%	14022	13.56%	96	74.05%	463	90.97%	1634	31.32%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront	0	100.00%	1	99.84%	0	100.00%	1	99.86%	0	100.00%	80	96.05%		
MWTI eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		3
Norman Virus Control	7	99.94%	0	100.00%	269	99.29%	9	98.48%	0	100.00%	710	82.17%	3	
PCTools Anti-Virus	0	100.00%	2	99.89%	22	99.58%	8	98.86%	0	100.00%	221	84.99%		
PCTools Spyware Doctor	0	100.00%	2	99.89%	42	99.78%	8	98.86%	3	99.93%	220	85.05%	1	
Quick Heal Quick Heal	0	100.00%	0	100.00%	1035	95.18%	17	96.59%	73	98.23%	1130	73.04%		
Redstone Redprotect	1	99.86%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		1
Rising Antivirus	1	99.97%	6	99.44%	10993	41.26%	51	90.30%	1273	69.32%	1327	46.17%	2	
Sophos Anti-Virus	4	99.96%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	8	99.61%		3
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Trend Micro OfficeScan	2	99.98%	3	99.89%	749	98.16%	9	98.67%	0	100.00%	738	84.88%		
VirusBuster VirusBuster	0	100.00%	2	99.89%	20	99.79%	8	98.86%	0	100.00%	220	85.05%		

Alwil avast! Professional 4.7.1075

ItW	100.00%	**Worms & bots**	99.69%
ItW (o/a)	100.00%	**DOS**	97.74%
File infector	100.00%	**Macro**	99.56%
Polymorphic	85.69%	**False positives**	1

Alwil's product is one of the more dependable regulars in *VB*'s tests, and while the interface is far from my favourite,

its intricacies no longer cause too many difficulties. Some admirably solid results were achieved on scanning the new archive set, with neither the archived nor the renamed copies of the Eicar test file spotted in the default modes, but everything detected with the archive and 'all files' settings switched on.

Speeds on demand were good, although on-access times were harder to come by – the product does not check files on simple opening, and on-access results for the infected sets were taken by copying the collection to the system across the network.

Results were pretty much as expected for *avast!*, with some older items missed but little from the more up-to-the-minute sets. Full coverage of the WildList was achieved, but hopes of a VB100 award were dashed by a single false positive in the clean set.

Avira AntiVir Windows Workstation 7.06.509

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.79%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.85%	**False positives**	2

AntiVir is another solid performer in *VB*'s comparative testing, with an excellent history both in detection and speed, and it did well again here.

The product is pleasingly laid out and simple to use, with the installer especially rapid and problem-free, and the tests zipped along at a similarly impressive rate. The archive sets were covered fully by default on demand, and almost so on access, with the rather odd exception of a few files in the .ACE format – while most were spotted, including the deepest nested to 10 levels, levels 3, 5 and 8 were missed.

Infected items were covered pretty well, with only a small number of polymorphic samples of rather rare and obscure variants missed. With the WildList test set covered in full, including those pesky Virut samples, only false positives could stop *Avira* claiming another award, and unluckily, two files were indeed erroneously flagged as infected, denying *Avira* the chance to add to its collection of VB100 awards this month.

BitDefender AntiVirus 2008

ItW	100.00%	**Worms & bots**	99.84%
ItW (o/a)	100.00%	**DOS**	99.79%
File infector	98.48%	**Macro**	99.98%
Polymorphic	100.00%	**False positives**	0

The *BitDefender* product stated that a better version of the *Windows Installer* was needed to install it – but as a pleasant surprise it also informed me that it had a copy handy and would install it for me. The pleasurable moment soon passed though, when after a reboot and a second attempt at installing, it was found that *IE6* would also be needed and on that count I would have to fend for myself.

I had also been informed that *Update Rollup 1* was required for the product to function – but a quick check without this generated no warnings from the product, and left the on-access functionality crippled, despite a comforting green tick insisting that all protection was active.

After several reboots therefore, I was finally able to get to work, and initial scans proceeded quite happily, with no false positives spotted on demand and most of the archive types detected easily, although .TGZ and self-extracting zips were only delved into to a depth of eight levels.

Scanning of the infected sets proved simple and highly successful, with a tiny number of misses and no false positives, thus earning *BitDefender* another VB100 award.

Bullguard Bullguard 8.0-32bit

ItW	100.00%	**Worms & bots**	99.84%
ItW (o/a)	100.00%	**DOS**	99.79%
File infector	98.48%	**Macro**	99.98%
Polymorphic	100.00%	**False positives**	0

Installing *Bullguard* confirmed a suspicion I had had all along – that the requirement for upgrades to *Internet Explorer* (already made by a few products and likely to crop up at least a few more times before I was done) is purely for cosmetic reasons. *Bullguard* has no such dependency, and installed smoothly on the bare system with no need for any extra work on my part.

The user experience was not adversely affected by the lack of modern display technology, and the tests proceeded nicely, recording similar times and detection rates to *BitDefender*, whose engine the product is based on.

The archive results were likewise the same, with .TGZ and self-extractors limited to eight levels but everything else covered. With admirable detection rates – missing barely a handful of samples per set, none of which were in the WildList set – and no false positives, *Bullguard* earns its second VB100.

On-access tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
AEC Trustport Antivirus	7	99.94%	0	100.00%	92	99.59%	2	99.24%	0	100.00%	553	89.53%		
Agnitum Outpost	0	100.00%	3	99.74%	28	99.58%	10	98.11%	0	100.00%	220	84.18%		
Alwil avast!	0	100.00%	7	99.69%	757	97.74%	0	100.00%	18	99.56%	657	85.69%	1	
Avira AntiVir	0	100.00%	0	100.00%	32	99.79%	0	100.00%	0	100.00%	3	99.85%	2	
BitDefender AntiVirus	0	100.00%	1	99.84%	8	99.79%	2	98.48%	2	99.96%	0	100.00%		
Bullguard Bullguard	0	100.00%	1	99.84%	8	99.79%	2	98.48%	1	99.98%	0	100.00%		
CA Antivirus	20	99.18%	0	100.00%	235	99.70%	3	99.02%	0	100.00%	9	99.60%		
CA eTrust	0	100.00%	0	100.00%	235	99.70%	3	99.02%	12	99.82%	9	99.60%		
Doctor Web Dr.Web	11	98.50%	1	99.84%	0	100.00%	2	99.24%	0	100.00%	0	100.00%	2	
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%		
Fortinet Forticlient	2	99.98%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	99.90%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%		
F-Secure Anti-Virus 2008	0	100.00%	1	99.84%	0	100.00%	2	99.24%	0	100.00%	1	99.91%		1
GDATA Anti-virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		2
Grisoft AVG	0	100.00%	6	99.84%	200	98.96%	9	96.97%	3	99.93%	695	76.07%		
Ikarus Virus Utilities	9	99.88%	8	99.68%	2461	91.37%	21	94.13%	171	96.07%	353	80.58%	13	31
Iolo Antivirus	34	99.69%	1	99.84%	0	100.00%	2	99.24%	0	100.00%	4	99.83%		
Kaspersky Anti-Virus	1	99.86%	0	100.00%	0	100.00%	2	99.24%	0	100.00%	1	99.91%		
Kingsoft AntiVirus	60	95.63%	600	18.23%	14022	13.56%	96	74.05%	463	90.97%	1634	31.32%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront	0	100.00%	1	99.84%	0	100.00%	3	99.10%	0	100.00%	80	96.05%		
MWTI eScan	0	100.00%	1	99.84%	0	100.00%	0	100.00%	0	100.00%	1	99.91%		2
Norman Virus Control	7	99.94%	0	100.00%	269	99.29%	11	97.73%	0	100.00%	867	76.84%	3	
PCTools Anti-Virus	0	100.00%	4	99.72%	22	99.58%	10	98.11%	0	100.00%	221	84.99%		
PCTools Spyware Doctor	0	100.00%	2	99.89%	42	99.78%	8	98.86%	3	99.93%	220	85.05%	1	
Quick Heal Quick Heal	0	100.00%	0	100.00%	1088	91.07%	18	96.02%	73	98.23%	1130	73.04%		
Redstone Redprotect	1	99.86%	0	100.00%	0	100.00%	2	99.24%	0	100.00%	1	99.91%		1
Rising Antivirus	2	99.96%	9	98.97%	10993	41.26%	53	89.55%	1273	69.32%	1327	46.17%	1	
Sophos Anti-Virus	4	99.96%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	8	99.61%		
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Trend Micro OfficeScan	2	99.98%	3	99.89%	749	98.16%	9	98.67%	0	100.00%	738	84.88%		
VirusBuster VirusBuster	0	100.00%	4	99.72%	20	99.79%	10	98.11%	0	100.00%	220	85.05%		

CA Antivirus 9.0.0.143

ItW	99.18%	**Worms & bots**	100.00%
ItW (o/a)	99.18%	**DOS**	99.70%
File infector	99.77%	**Macro**	100.00%
Polymorphic	99.60%	**False positives**	0

A few hiccups occurred during the installation of *CA*'s home-user product, starting with the seemingly inevitable need to upgrade the browser (a minimum of version 5.5 this time). I also noted that some other items come along with the product, including the *Yahoo! Toolbar*, and that the browser homepage was set to *Yahoo!*, which I found rather surprising. I was positively upset by the fact that the boxes

to accept these changes were checked by default – since the VB100 testing protocol requires default settings, this meant agreeing to yet more EULAs, which in traditional *CA* style must be scrolled all the way through before they can be accepted.

The design of the product itself is pretty slick, with clear and easy controls, and despite my misgivings about the optional extras I found myself quite liking it. Configuration was fairly minimal, but the defaults made sense, with archive scanning switched on for on-demand scanning (.ACE files not scanned) and off for on-access scanning except for a single level of the ubiquitous .ZIP (and its twin sister .JAR, essentially zip renamed).

Scanning speeds were very good indeed, and detection generally good, but in the WildList set several items were missed including some W32/Rbot variants and the entire set of the W32/Viruts. *CA* thus misses out on a VB100 award here.

CA eTrust 8.1.637.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.70%
File infector	99.02%	**Macro**	99.82%
Polymorphic	99.60%	**False positives**	0

CA's more grown-up product, the corporate-targeted *eTrust*, did not complain about the browser in use during the installation, but I found myself needing to upgrade regardless when I later found that some of the popup screens in the options areas of the interface lacked their vital control buttons.

This interface has never been a favourite of mine, but its usual slowness under *Windows XP* was somewhat less intrusive under *2000*. Accessing logs was as tricky as ever, with large ones occasionally overwhelming the display system and leaving me with blank browser windows and no option to export to a text file. As usual I simply removed the raw files to a *Linux* machine and stripped out the required data.

The logs indicated much better coverage of the WildList by *eTrust* than by its sister product, hinting that the home-user product submitted may have been using some slightly older definition data. Archive scanning was a little odd, with a maximum of nine levels checked on demand and none on access, despite the GUI inferring that they should be. Speeds were very good, and without any false positives *eTrust* succeeds where *CA AV* failed, and wins another VB100 award.

Doctor Web Dr.Web 4.44.0

ItW	98.50%	**Worms & bots**	99.84%
ItW (o/a)	98.50%	**DOS**	100.00%
File infector	99.24%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	2

Dr.Web proved much less problematic, with a simple installer requiring no extra fiddling and another very pleasing interface, laid out with impressive clarity and logic as well as being appealing to the eye. Running through the tests was quite enjoyable as a result, which was a good thing as they did take some time – *Dr.Web* is a very thorough product, delving deeply into files before passing them as clean. On demand, archives were not scanned by default. However, .CHM help files, of which a few are included in the clean set, are checked in all their many sub-parts, which explains the relatively low throughput, rendered even lower when full archive scanning is activated. Full archive scanning covered everything but .ACE to a depth of 10 levels.

Detection rates were excellent across the test sets until the WildList tripped the product up with several misses, including those pesky W32/Virut samples. A couple of false positives added to *Dr.Web*'s problems, and the product unfortunately misses out on a VB100 once more.

ESET NOD32 2.70.39

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.95%	**False positives**	0

Nod32 has undergone a bit of a revolution recently, with a spanking new interface introduced to coincide with the launch of version 3, and that of its big sister *Smart Security* (see *VB*, November 2007, p.19). However, *ESET* opted to give the ever-reliable version 2.7 one last hurrah this month.

Installing and using the product has never been too difficult, and as usual testing sped through in remarkable time, with the usual excellent results. Speeds were as fast as ever, although archives could not be scanned on access, and detection was at the expected near flawless level, with only a single rather obscure and highly polymorphic sample missed. With the WildList fully covered and no false positives, *ESET* adds yet another VB100 award to its groaning trophy cabinet.

On-demand throughput	Archive files - default		Archive files - all files		Binaries and system files - default		Binaries and system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - default	
	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
AEC Trustport Antivirus	4929	0.6	4929	0.6	3157	0.9	3157	0.9	255	5.7	255	5.7	387	1.8	387	1.8
Alwil avast!	20	151.4	812	3.7	194	14.0	223	12.2	22	66.0	57	25.5	18	38.0	43	15.9
Avira AntiVir	616	4.9	650	4.7	100	27.1	99	27.4	25	58.1	30	48.4	19	36.0	36	19.0
BitDefender AntiVirus	1051	2.9	1051	2.9	342	7.9	342	7.9	51	28.5	51	28.5	54	12.7	54	12.7
Bullguard Bullguard	1054	2.9	1054	2.9	318	8.5	318	8.5	64	22.7	64	22.7	67	10.2	67	10.2
CA Antivirus	761	4.0	761	4.0	93	29.2	93	29.2	32	45.4	32	45.4	23	29.8	23	29.8
CA eTrust	466	6.5	466	6.5	70	38.8	70	38.8	28	51.9	28	51.9	20	34.2	20	34.2
Doctor Web Dr. Web	637	4.8	3230	0.9	487	5.6	604	4.5	93	15.6	92	15.8	88	7.8	100	6.8
ESET NOD32	9	336.5	877	3.5	55	49.4	434	6.3	36	40.4	39	37.2	26	26.3	32	21.4
Fortinet Forticlient	471	6.4	471	6.4	494	5.5	494	5.5	27	53.8	27	53.8	45	15.2	45	15.2
Frisk F-PROT	192	15.8	192	15.8	245	11.1	245	11.1	32	45.4	32	45.4	21	32.6	21	32.6
F-Secure Anti-Virus	2218	1.4	2388	1.3	236	11.5	235	11.6	80	18.2	80	18.2	24	28.5	83	8.2
GDATA Anti-virus	2609	1.2	2609	1.2	418	6.5	418	6.5	86	16.9	86	16.9	83	8.2	83	8.2
Grisoft AVG	1130	2.7	2826	1.1	381	7.1	392	6.9	119	12.2	155	9.4	81	8.4	279	2.5
Ikarus Virus Utilities	200	15.1	N/A	N/A	244	11.1	N/A	N/A	50	29.1	N/A	N/A	65	10.5	N/A	N/A
Iolo Antivirus	237	12.8	246	12.3	249	10.9	251	10.8	19	76.5	27	53.8	21	32.6	40	17.1
Kaspersky Anti-Virus	2061	1.5	2061	1.5	403	6.7	403	6.7	90	16.1	90	16.1	81	8.5	81	8.5
Kingsoft AntiVirus	828	3.7	828	3.7	248	10.9	248	10.9	63	23.1	63	23.1	74	9.3	74	9.3
McAfee VirusScan	50	60.6	821	3.7	288	9.4	301	9.0	49	29.6	49	29.6	59	11.6	82	8.3
Microsoft Forefront	939	3.2	939	3.2	276	9.8	276	9.8	62	23.4	62	23.4	40	17.1	40	17.1
MWTI eScan	1832	1.7	1832	1.7	432	6.3	432	6.3	297	4.9	297	4.9	298	2.3	298	2.3
Norman Virus Control	905	3.3	905	3.3	1368	2.0	1368	2.0	46	31.6	46	31.6	150	4.6	150	4.6
PCTools Anti-Virus	397	7.6	704	4.3	1333	2.0	1339	2.0	1283	1.1	1285	1.1	1592	0.4	1595	0.4
PCTools Spyware Doctor	963	3.1	963	3.1	340	8.0	340	8.0	73	19.9	73	19.9	60	11.4	60	11.4
Quick Heal Quick Heal	730	4.1	767	3.9	91	29.8	95	28.6	61	23.8	67	21.7	18	38.0	36	19.0
Redstone Redprotect	1717	1.8	1827	1.7	304	8.9	304	8.9	166	8.8	166	8.8	162	4.2	162	4.2
Rising Antivirus	1564	1.9	1564	1.9	357	7.6	357	7.6	63	23.1	63	23.1	56	12.2	56	12.2
Sophos Anti-Virus	53	57.1	1020	3.0	197	13.8	244	11.1	27	53.8	44	33.0	16	42.8	54	12.7
Symantec Endpoint Protection	684	4.4	684	4.4	218	12.5	218	12.5	64	22.7	64	22.7	63	10.9	63	10.9
Trend Micro OfficeScan	124	24.4	125	24.2	180	15.1	181	15.0	27	53.8	27	53.8	32	21.4	40	17.1
VirusBuster VirusBuster	533	5.7	695	4.4	211	12.9	212	12.8	29	50.1	47	30.9	19	36.0	40	17.1

Fortinet Forticlient 3.0.470

ItW	99.98%	**Worms & bots**	100.00%
ItW (o/a)	99.98%	**DOS**	100.00%

File infector	100.00%	**Macro**	100.00%
Polymorphic	99.90%	**False positives**	0

Fortinet's desktop product remains little changed since I first encountered it, presenting a serious-looking interface

with a wealth of security functions accessed via a string of tabs. During installation the product complained about a missing DLL file, but presumably this related to some other part of the product, as the anti-virus seemed as solid and robust as ever.

Usability was similarly problem-free, and scanning times were decent for the level of thoroughness offered by the default settings, detecting the majority of the nested archives without the need for adjustment.

Detection was splendid almost across the board until those troublesome Virut samples reared their ugly heads, with two missed detections being enough to prevent *Fortinet* from winning another VB100 award.

Frisk F-PROT Anti-virus

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.95%	**False positives**	1

F-PROT is perhaps the simplest product on test this month, with a fairly basic interface providing access to straightforward anti-virus scanning and cleaning and no additional bells and whistles. This made testing pretty straightforward, and everything zoomed through in good time, with the more in-depth speed tests skipped on access thanks to a dearth of configuration.

Detection was as top-class as ever, with just about everything taken in the engine's stride, but a single false positive showed up in the clean set, a file apparently highly similar to a known malicious item, meaning that *Frisk* joins the growing list of vendors narrowly failing to reach the VB100 standard this month.

F-Secure Anti-Virus 2008

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.91%	**False positives**	0

F-Secure's current product is another highly familiar one which took little time to get set up and going.

The in-depth scanning with multiple technologies meant speed times were not the best, even though archives could not apparently be scanned deeper than five levels. While running sizeable scans, the interface choked up a few times, lingering unresponsive at the very last stage of the scanning process, with only a reboot able to bring it back in touch with the user. Logging was also a little pesky, with sizeable chunks of information apparently missing from logs exported from the viewer interface.

However, detection was excellent, and there were no false detections, and *F-Secure* thus comfortably earns another VB100 award.

GDATA Anti-virus 18.0.7295.201

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.91%	**False positives**	0

GDATA's product is another multi-engine beast, which for this submission at least seems to have dropped the familiar '*AVK*' name. The interface seemed unchanged however – a clear and well-laid-out thing which is always a pleasure to operate.

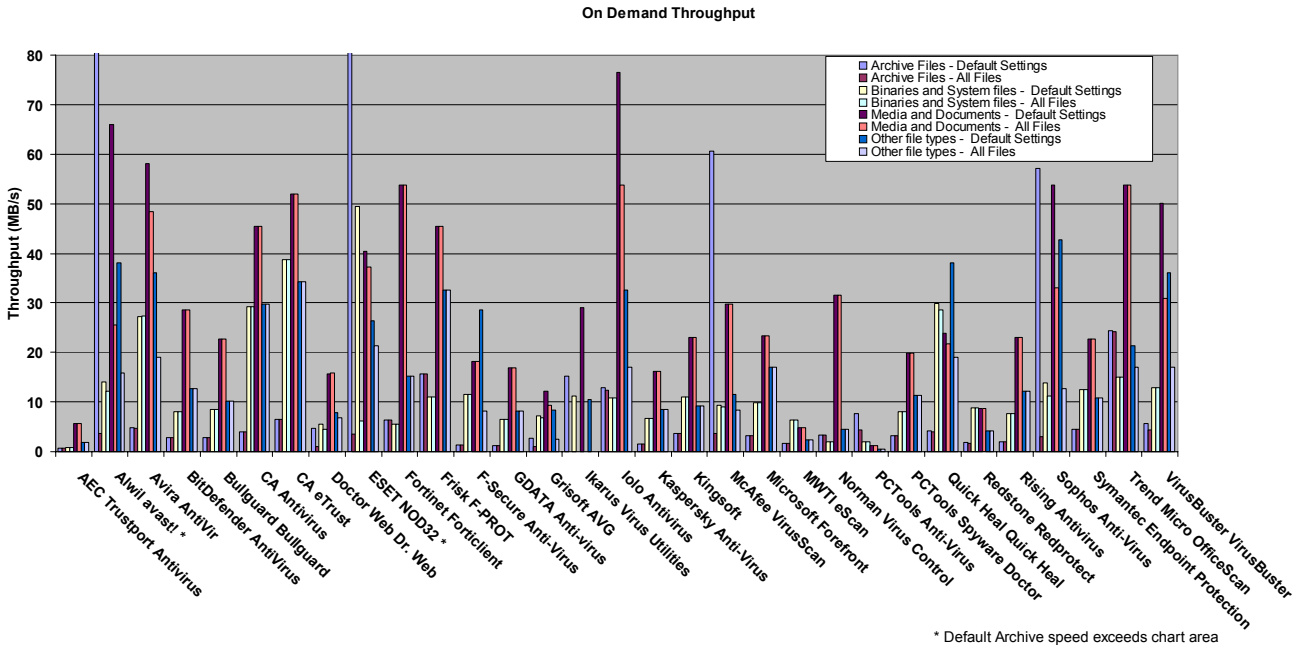
Of course, the multiple engines meant that scanning speeds were slow, even on access, but depth of scanning and accuracy are clearly the product's strengths, and with barely any misses and no false positives *GDATA* also wins a VB100 award for its collection.

Grisoft AVG 7.5.503

ItW	100.00%	**Worms & bots**	99.86%
ItW (o/a)	100.00%	**DOS**	98.96%
File infector	97.73%	**Macro**	100.00%
Polymorphic	76.07%	**False positives**	0

Wildly popular *AVG*, the free home-user version of which seems to be in almost every home these days, has always been a little fiddly for my liking, but whether it has been tweaked a little or I've just grown used to it, in this test I found the interface perfectly reasonable and even quite pleasant to work with.

Configuration was a little short for the on-access scanner, but elsewhere everything worked fine, with very good if not great detection in the infected sets, including flawless coverage of the WildList despite those difficult polymorphic samples. With no false positives either, *Grisoft* also wins another VB100 award.



* Default Archive speed exceeds chart area

Ikarus Virus Utilities 1.0.60

ItW	99.88%	**Worms & bots**	99.81%
ItW (o/a)	99.88%	**DOS**	91.37%
File infector	93.37%	**Macro**	96.07%
Polymorphic	80.58%	**False positives**	13

Ikarus has had some problems in its recent entries in VB100 comparative reviews, but earlier issues with its interface seem to have been resolved – on this occasion everything ran fine and stably with no difficulty. Even the updates to the *Windows Installer* and the .NET framework required by the product were provided thoughtfully as part of the submission and installed automatically as part of the setup process.

Configuration of scanning is somewhat limited by the interface, but the default setting of scanning up to three levels into archive files seems sensible, and speeds were fairly good across the sets.

Detection was a little improved on previous efforts, but a handful of samples of each of two Virut variants in the set proved undetectable, and a rash of false positives added to *Ikarus*'s woes. There were also a fair number of items labelled 'not-a-virus: Monitor.Win32.Keylogger', which for now I have generously recorded as 'suspicious' rather than full false positive detections, but which certainly seem a little suspect themselves.

Despite these problems the product seems to be improving fast and looks a likely candidate to qualify for a VB100 award sometime soon.

Iolo Antivirus 1.1.15

ItW	99.71%	**Worms & bots**	99.84%
ItW (o/a)	99.69%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.83%	**False positives**	0

Iolo returns to the test bench for another stab after being denied a VB100 by a whisker a few months ago. The product is well designed and pleasant to use, and although it requires *IE6* to operate, it politely offers to go online and fetch a copy.

As with many of the products aimed more squarely at the home user, configuration was somewhat limited, with on-access scanning barely adjustable and actions on discovering malware restricted to delete, disinfect or quarantine. With logging also absent, I allowed the product to delete the virus collections from the system, which left only a few samples in most sets but also many of the two Virut strains along with another file infector, W32/Expiro. *Iolo* will therefore have to try again for the VB100 award, which should be well within its grasp with just a little more work.

Kaspersky Anti-Virus 7.0.0.125

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	99.86%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.91%	**False positives**	0

Kaspersky is a much more seasoned product, version 7 of the product having dropped a lot of the cuddly cartoonishness of the previous offering and presenting a sterner but glossier face to the world. Usability has not been diminished however, and few problems were encountered other than some slowness exporting particularly large logs to file.

Detection rates were excellent as ever, with the new nested set detected very neatly. With no false positives spotted, all looked good until a single item was missed on access. This, an instance of W32/Autorun added recently to the list, could be detected by the product on demand, but was not scanned on access unless the 'scan installation packages' option was activated. *Kaspersky* thus narrowly misses out on a VB100 award this time.

Kingsoft AntiVirus

ItW	95.63%	**Worms & bots**	18.23%
ItW (o/a)	95.63%	**DOS**	13.56%
File infector	74.05%	**Macro**	90.97%
Polymorphic	31.32%	**False positives**	0

Kingsoft achieved a VB100 award in its previous appearance in *VB* (see *VB*, August 2007, p.13). The product this time seemed little changed, with the interface nicely laid out and appearing pretty stable, but experiencing some difficulties in the log viewer when faced with unfamiliar locales – only US English is supported, and others cause a nasty crash.

Scanning speeds were rather average, and configuration absent on access, but false positives and even suspicious flags were encouragingly absent throughout the clean sets.

The infected sets were less well covered, in particular the older items, and in the WildList set several nasties were missed, including most of the files infected with Virut and Expiro, as well as several W32/SDbot variants. *Kingsoft* thus falls short of the required standard this time, and will have to try again to achieve its second VB100 award.

McAfee VirusScan Enterprise 8.50i

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

McAfee's desktop product is another that seems to have remained relatively unchanged for some time, and its performance was similarly predictable.

Scanning times were decent, with archives ignored by default in both modes but thoroughly handled if requested; detection was impeccable, with nothing missed anywhere and no false positives. *VirusScan* wins a VB100 award effortlessly.

Microsoft Forefront Client Security 1.5.1941

ItW	100.00%	**Worms & bots**	99.84%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	99.86%	**Macro**	100.00%
Polymorphic	96.05%	**False positives**	0

Perhaps unsurprisingly, *Forefront* makes use of all available *Microsoft* technology and requires numerous updates to be in place before it will install. The rollup package, an improved version of the installer, and an update to the Agent API are all required. It also uses the event log to record its activities rather than providing its own system, which I found a little awkward, but the server-side management system doubtless provides a more usable form of information management.

Configuration was rather minimal, which again may be explained by the absence of the management side of things, but defaults were sensible and testing ran without difficulties. With nothing of significance missed and no false positives, *Forefront* qualifies for a VB100 award.

MWTI eScan 9.0.747.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.91%	**False positives**	0

Microworld Technologies presents a fairly comprehensive product, including the *Kaspersky* engine alongside a range of its own protection technologies. The product's default settings lean towards the paranoid, with on-access defaults including all archive types. With a well designed interface providing for all my needs, testing thus took little of my own time, but quite a bit for the system, as clean sets were probed deeply.

Detection of the infected sets was excellent, *eScan* managing to avoid the problem which upset *Kaspersky*'s own product, and comfortably earning a VB100 award.

File access lag time	Archive files - default		Archive files - all files		Binaries and system files - default		Binaries and system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - all files	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
AEC Trustport Antivirus	1007	0.3	1007	0.3	328	0.1	328	0.1	98	0.1	98	0.1	129	0.2	129	0.2
Alwil avast!	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Avira AntiVir	28	0.0	112	0.0	95	0.0	127	0.0	24	0.0	35	0.0	15	0.0	43	0.1
BitDefender AntiVirus	114	0.0	N/A	N/A	259	0.1	259	0.1	53	0.0	53	0.0	58	0.1	58	0.1
Bullguard Bullguard	113	0.0	900	0.3	283	0.1	315	0.1	51	0.0	58	0.0	63	0.1	67	0.1
CA Antivirus	22	0.0	N/A	N/A	83	0.0	83	0.0	33	0.0	33	0.0	27	0.0	27	0.0
CA eTrust	19	0.0	N/A	N/A	73	0.0	73	0.0	33	0.0	33	0.0	26	0.0	26	0.0
Doctor Web Dr. Web	540	0.2	2050	0.7	480	0.2	908	0.3	84	0.1	84	0.1	81	0.1	87	0.1
ESET NOD32	12	0.0	N/A	N/A	63	0.0	63	0.0	42	0.0	42	0.0	33	0.0	33	0.0
Fortinet Forticlient	308	0.1	308	0.1	268	0.1	268	0.1	28	0.0	28	0.0	43	0.1	43	0.1
Frisk F-PROT	64	0.0	N/A	N/A	263	0.1	263	0.1	41	0.0	41	0.0	27	0.0	27	0.0
F-Secure Anti-Virus	36	0.0	1432	0.5	202	0.1	222	0.1	36	0.0	133	0.1	26	0.0	105	0.1
GDATA Anti-virus	222	0.1	1380	0.5	371	0.1	396	0.1	163	0.1	172	0.1	116	0.2	132	0.2
Grisoft AVG	18	0.0	N/A	N/A	130	0.0	130	0.0	22	0.0	28	0.0	10	0.0	29	0.0
Ikarus Virus Utilities	209	0.1	N/A	N/A	254	0.1	254	0.1	53	0.0	53	0.0	70	0.1	70	0.1
Iolo Antivirus	52	0.0	N/A	N/A	241	0.1	261	0.1	26	0.0	37	0.0	25	0.0	27	0.0
Kaspersky Anti-Virus	37	0.0	214	0.1	199	0.1	222	0.1	75	0.0	84	0.1	48	0.1	72	0.1
Kingsoft AntiVirus	59	0.0	N/A	N/A	229	0.1	229	0.1	71	0.0	71	0.0	80	0.1	80	0.1
McAfee VirusScan	48	0.0	479	0.2	284	0.1	295	0.1	47	0.0	47	0.0	58	0.1	58	0.1
Microsoft Forefront	90	0.0	N/A	N/A	273	0.1	273	0.1	77	0.0	77	0.0	40	0.0	40	0.0
MWTI eScan	999	0.3	999	0.3	218	0.1	218	0.1	80	0.1	80	0.1	73	0.1	73	0.1
Norman Virus Control	16	0.0	N/A	N/A	110	0.0	110	0.0	53	0.0	53	0.0	74	0.1	74	0.1
PCTools Anti-Virus	345	0.1	N/A	N/A	890	0.3	N/A	N/A	123	0.1	N/A	N/A	97	0.1	N/A	N/A
PCTools Spyware Doctor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Quick Heal Quick Heal	14	0.0	N/A	N/A	81	0.0	N/A	N/A	37	0.0	N/A	N/A	15	0.0	N/A	N/A
Redstone Redprotect	43	0.0	1448	0.5	227	0.1	259	0.1	112	0.1	115	0.1	91	0.1	96	0.1
Rising Antivirus	55	0.0	N/A	N/A	327	0.1	327	0.1	64	0.0	64	0.0	62	0.1	62	0.1
Sophos Anti-Virus	31	0.0	1011	0.3	204	0.1	228	0.1	35	0.0	36	0.0	21	0.0	49	0.1
Symantec Endpoint Protection	24	0.0	N/A	N/A	216	0.1	N/A	N/A	35	0.0	N/A	N/A	33	0.0	N/A	N/A
Trend Micro OfficeScan	1052	0.3	1052	0.3	930	0.3	930	0.3	40	0.0	40	0.0	43	0.1	43	0.1
VirusBuster VirusBuster	31	0.0	N/A	N/A	214	0.1	215	0.1	27	0.0	45	0.0	15	0.0	40	0.0

Norman Virus Control v.5.9

ItW	99.94%	**Worms & bots**	100.00%
ItW (o/a)	99.94%	**DOS**	99.29%
File infector	98.48%	**Macro**	100.00%
Polymorphic	82.17%	**False positives**	3

Norman's is another interface which has grown on me after struggling to understand its complexities in earlier tests. The

only lingering annoyance is the lack of information on scan progress, with there being no progress bar or count of files scanned so far.

Speeds were reasonable, and detection levels decent, with most misses on old and obscure items. However, two files in the clean sets were flagged as nondescript malware by the heuristics, thanks to the use of a rather unusual packer, and again some of those tricky Virut samples were missed, leaving *Norman* just short of the mark for the VB100 award this month.

PCTools Anti-Virus 3.6.1.7

ItW	100.00%	**Worms & bots**	99.89%
ItW (o/a)	100.00%	**DOS**	99.58%
File infector	98.86%	**Macro**	100.00%
Polymorphic	84.99%	**False positives**	0

PCTools is a relative newcomer to VB100 comparative testing, taking its first award just a few months ago (see *VB*, June 2007, p.10).

The plain anti-virus product, based on the *VirusBuster* engine, offers a reasonable level of configuration and a pleasant user experience for the most part. The logging presented rather a strange problem though – opening logs from the interface brought up a 'file in use' error, and they could thus only be accessed by copying the files and opening the copies.

Some good detection rates were shown, but also some remarkably slow times in the speed tests, even with the default on-demand settings scanning archives to a depth of one level only. However, with nothing missed in the WildList and no false positives, *PCTools AV* wins itself a second VB100 award.

PCTools Spyware Doctor 5.1.0.272

ItW	100.00%	**Worms & bots**	99.89%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	98.86%	**Macro**	99.93%
Polymorphic	85.05%	**False positives**	1

Spyware Doctor is *PCTools*' rather more venerable anti-spyware product, now available with anti-virus functionality rolled in, and while the interface closely resembles the plain AV product there were a number of differences.

Logging seemed to be limited to a small file size, meaning that larger scans needed to be split up into chunks to acquire the necessary data, while on-access scanning seemed not to be sparked by simple file opening, which meant the product had to be excluded from the on-access speed test.
On-demand times were considerably better than those of its sister product, despite defaults including all archive types (apart from the rather obscure .LZH) to a depth of at least 10 levels.

Detection rates differed slightly too, and in the clean set the anti-spyware side of things detected a single false positive, thus denying *Spyware Doctor* a VB100 despite full coverage of the WildList.

Quick Heal Quick Heal AntiVirus Lite 9.50

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	95.18%
File infector	96.59%	**Macro**	98.23%
Polymorphic	73.04%	**False positives**	0

Quick Heal (which is now the name of both the product and its vendor, having recently changed from *CAT*) is another well designed product.

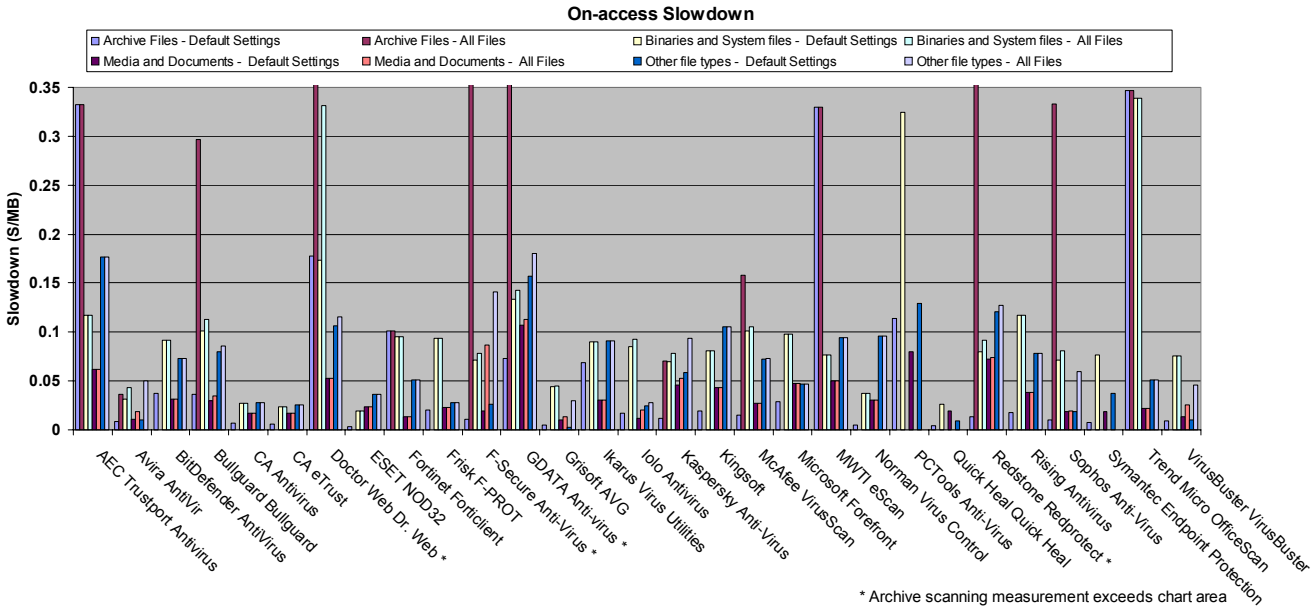
It zipped through speed tests in good time and could only be cajoled into scanning to a depth of five levels, into a limited selection of archive types. A few nasty crashes occurred during the scanning of infected sets, but they were handled better on a second attempt, and while detection was a little short on the older sets nothing more important was missed, and false positives were also absent. *Quick Heal* thus earns itself a VB100 award.

Redstone Redprotect 0.4.1.27681

ItW	99.86%	**Worms & bots**	100.00%
ItW (o/a)	99.86%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.91%	**False positives**	0

UK-based *Redstone* produces a managed-service protection product, of which this is a simple client version using the .NET framework for its interface. Running the product is a straightforward business, with a simple menu accessed via the system tray. Configuration is a little more fiddly, requiring the tweaking of registry settings, but the submission came with a prepared set of useful entries, enabling testing to proceed without too many problems.

The product is based on the *Kaspersky* engine, and detection rates were thus at the top end of the scale, while speed times were more average. A few difficulties were encountered,



including the absence of logging and some odd behaviour on demand, when the 'always delete' option seemed to be ignored for a few items, resulting in a string of popups requesting confirmation before deleting.

False positives were absent, but the W32/Autorun sample which tripped up *Kaspersky* was also missed here, in both modes, and *Redstone* will thus have to try again before gaining a VB100 award.

Rising Antivirus 2008 20.15.32

ItW	99.97%	**Worms & bots**	99.44%
ItW (o/a)	99.96%	**DOS**	41.26%
File infector	90.30%	**Macro**	69.32%
Polymorphic	46.17%	**False positives**	2

Another newcomer to the VB100 test bench, China-based *Rising* has developed a considerable profile outside its home country in recent years, and it was with some excitement that I took my first look at its product. First impressions were excellent, with the product looking very clean and stylish, clearly laid out and easy to use.

Speed test results were fairly good, and stability seemed solid too, but during on-access scanning of the infected sets the product seemed to stop blocking after 10,000 samples or so. The test was retried at a slower pace. The problem did not recur, and results were thus obtained, showing the expected high numbers of misses in older sets but little in the newer areas. Two misses in the WildList, both single samples from sets of file-infectors, and a pair of false positives in the clean sets, were enough to spoil *Rising*'s chances of qualifying for the VB100 at first attempt, but it is another likely candidate to make the grade pretty soon.

Sophos Anti-Virus 7.03

ItW	99.96%	**Worms & bots**	100.00%
ItW (o/a)	99.96%	**DOS**	100.00%
File infector	100.00%	**Macro**	99.80%
Polymorphic	99.61%	**False positives**	0

Sophos is among the most regular of VB100 entrants, with its product little changed in the half-dozen *Windows* tests I have performed in my time here, and as usual setting it up and running the tests were simple tasks. Speeds were very good, even with archive scanning turned up to the maximum available five levels, and after a false positive upset things last time (see http://www.virusbtn.com/vba/2007/10) the clean sets were cleared with only a few hacker tools alerted on as possible security risks.

Detection was at its usual high levels, with almost everything covered, but again in the WildList set those Virut samples proved too difficult, and *Sophos* is denied the VB100 for the second time in a row.

Symantec Endpoint Protection 11.0.780.1109

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

This month *Symantec* presented a totally different looking product from those seen in previous tests, considerably more colourful and less severe. The cosmetic enhancements required *IE6*, and after the installer had aborted requesting this update it left something lingering behind, which meant the *IE6* installer insisted on a reboot before it could run itself. However, after several reboots to set up, tests continued apace.

Speeds were reasonable, although configuration was somewhat less in-depth than in previous submissions and archives could only be scanned to a depth of three levels, with .ACE and .TGZ ignored. However, detection was excellent, with nothing missed, and without false positives either *Symantec* earns another VB100 award.

Trend Micro OfficeScan Client 8.0

ItW	99.98%	**Worms & bots**	99.89%
ItW (o/a)	99.98%	**DOS**	98.16%
File infector	98.67%	**Macro**	100.00%
Polymorphic	84.88%	**False positives**	0

OfficeScan also required *IE6* in order to operate the web console which provides much of the product's configuration, although options were available to delegate some control to the simpler local interface.

Testing slipped rapidly along, flipping between the two control systems as required, and times were good and detection rates decent, although the renamed Eicar test file was not spotted with the default settings. Some older sample sets were a little short, but more seriously two Virut samples were missed, one each of the two variants causing most trouble here, and *Trend* is thus denied an award this time.

VirusBuster VirusBuster Professional 5.3 Build 39

ItW	100.00%	**Worms & bots**	99.89%
ItW (o/a)	100.00%	**DOS**	99.79%
File infector	98.86%	**Macro**	100.00%
Polymorphic	85.05%	**False positives**	0

Bringing up the alphabetical rear, *VirusBuster* presented its usual colourful and reasonably usable product, which provided adequate configuration options and its usual slightly fiddly system of setting up scanning jobs. These jobs showed good scanning speeds, and pretty thorough detection across the sets; with those troublesome Virut variants taken in its stride, and without any sign of a false positive *VirusBuster* takes home another VB100 award.

CONCLUSIONS

Having expected numerous problems to have arisen from the aging platform, these proved to be limited to the chore of installing extras before products could install or operate properly.

In fact, far more difficulties were thrown up by another rather old issue, the polymorphic file-infecting virus. With modern malware trends having tended for some time towards the non-self-replicating, or at least towards static worms which simply drop identical copies of themselves around the place, old-style file infectors have been making something of a comeback lately. W32/Detnat, W32/Looked (aka Viking), W32/Fujacks, and of course the more tricky polymorphic type, W32/Polip and W32/Virut, all lurk on the WildList and some of them have made a considerable impression on global prevalence charts in recent months. This month's Virut addition revealed deficiencies in detection for several products, the vendors of which have all been informed of the problem, which should have been resolved by most in advance of the publication of this review.

A swathe of products have also fallen to another problem which has shown a rising trend lately: false positives. A relatively small addition to the clean test sets threw up several individual examples (few of the files that were false alarmed on affected more than one product, or more specifically one engine), and in some cases several files were misidentified by a single product.

The result has been one of the poorest scores for some time in a *VB* comparative, with fewer than half the entrants making the grade, and another trend – the inclusion of third-party engines in products – magnifying the scale of the problem. Hopefully the shock of so much devastation caused by a few polymorphic viruses will ensure virus labs remain on their guard and encourage more thorough checking of detection for file-infecting items in future.

Technical details

Test environment: Tests were run on identical machines with *AMD Athlon64 3800+* dual core processors, 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, all running *Microsoft Windows 2000 Professional SP4*.

Agnitum Outpost was tested on a 1.6 GHz *Intel Pentium* machine with 512 MB RAM and is thus excluded from speed measurements.