COMPARATIVE REVIEW

VB100 MARCH 2008 – WINDOWS VISTA BUSINESS EDITION SP1

John Hawes

Windows Vista makes another appearance on the *VB* test bench just over a year after its debut (see *VB*, February 2007, p.14) and eight months after a slightly less well-attended review of products on its 64-bit version (see *VB*, August 2007, p.16). During that time the platform has failed to make enormous headway in the marketplace, with most estimates reckoning it resides on at most 10% of the world's desktops, languishing far behind the dominant *XP*, which is thought still to hold sway on around 75% of systems.

The release of the first service pack for an operating system is often seen as a sign of maturity though, and SP1 for *Vista* could signal an upturn in the uptake of the platform. The upgrade promises a raft of improvements to performance and general functionality.

SP1 was released shortly after the deadline for product submissions for this review. With at least some participants not yet able to get their hands on a copy for testing, even more than the usual number of bugs and unpredictable behaviours were expected, and with one of the largest sets of products yet seen on the VB100 test bench, I anticipated an arduous slog through the tests this month.

Initially a total of 40 products were submitted on the February 28th deadline. Many of these were new to the tests, including a pair of products based on the open-source *ClamAV* detection technology, which promised to provide some interesting results. Several others returned after lengthy absences, and all the usual suspects were also present. With such a huge number of products to get through I decided that any which could not be made to provide usable results after the standard three installs would have to be shelved.

I also decided to streamline the results reporting process somewhat, if only to make the figures readable on the page. Thus, exact numbers of missed samples will not be reported in this month's comparative. As always, the percentages listed in the detection table represent the number of variants covered (or not) by the products, rather than the number of unique samples.

PLATFORM AND TEST SETS

Installation and set-up of *Vista* has become a fairly familiar process, and while the prettification of the install process itself always impresses me, my first act on seeing the garish, flashy interface is invariably to roll it back to its 'classic' appearance, which seems much less intrusive over long periods of exposure. Doubtless the glitzy 'Aero' look can be tweaked into something less nauseating, but this was not a process I was ready to spend any time on.

Application of the service pack was less painful than I had feared. Once installed, it seemed to make no obvious difference to the way things ran, although I did notice considerably fewer crashes and blue-screens than in previous tests. As in those earlier runs a user with minimal rights was created, to measure integration with user access controls and so on, but I expected to have to switch to the admin user or even disable UAC entirely for some products.

The clean test sets saw a fairly substantial enlargement, with most of the sets used for speed measurement now fast approaching a good size for freezing. This will enable more useful comparisons of product speeds over time as platforms are revisited (assuming the test hardware manages to withstand the heavy usage). An especially large number of additions were made to the polymorphic sets, thanks to there having been numerous misses in those areas in recent months – the variants of W32/Virut which have already been known to cause widespread problems are now more fully represented, and this should continue to tax the participants' detection abilities to the utmost.

The deadline for the test sets was February 25th, and with the January WildList having been available for a few weeks by then the WildList set was synchronized with that list. This meant a fairly large number of additions, but as the previous list saw some clearing out of older items the total number of variants in the core set remained around the usual level. The additions were dominated as usual by worms and bots such as W32/Ircbot and W32/Agent, with another handful of variants of W32/Virut and other nasty file infectors also joining the set for the first time.

I had hoped that this month would see the inclusion of a preliminary set of non-replicating malware, having spent some time gathering, validating and categorising new samples for this purpose. As a step towards this significant change, much of the older part of the test set has been moved aside into a 'legacy' set, as a precursor to the eventual retirement of all older items. With the unexpectedly high turnout of products, and some unforeseen delays in getting the lab ready for testing, the final stages of implementing the new trojan set had to be put on hold. Pared-down selection was included in the test out of interest and to gather data for name-referencing, and a further expanded version of the set should be ready in time for the next review. Even without this new challenge, the potential both for false positives and incomplete detection of polymorphic items was increased considerably and it

Detection rates on demand (OD) and on access (OA)	WildList viruses		Worms & bots		File infector viruses		Polymorphic viruses		Legacy samples		Clean sets	
	OD	OA	OD	OA	OD	OA	OD	OA	OD	OA	FP	Susp.
AEC Trustport Antivirus	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	86.39%	86.39%	97.62%	97.62%		
Agnitum Outpost Security Suite Pro	99.99%	99.99%	100.00%	100.00%	99.21%	99.21%	79.29%	79.29%	99.98%	99.98%		2
Ahnlab V3	100.00%	99.90%	99.76%	99.76%	99.21%	99.21%	88.06%	88.06%	96.77%	96.77%		
Alwil avast!	99.83%	99.83%	100.00%	100.00%	100.00%	100.00%	86.20%	86.20%	97.02%	97.02%	1	
AVG	100.00%	100.00%	100.00%	100.00%	98.43%	98.43%	73.89%	73.89%	97.63%	97.63%		
Avira AntiVir	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	84.68%		
BitDefender AntiVirus 2008	99.996%	99.996%	100.00%	100.00%	98.95%	98.95%	100.00%	100.00%	99.59%	99.59%		
Bullguard	99.996%	99.996%	100.00%	100.00%	98.95%	98.95%	100.00%	100.00%	99.59%	99.59%		
CA eTrust Antivirus	100.00%	100.00%	100.00%	100.00%	99.84%	99.84%	99.70%	99.70%	99.10%	99.10%		
CA Internet Security	100.00%	100.00%	100.00%	100.00%	99.84%	99.84%	99.70%	99.70%	99.10%	99.10%		
Check Point Zone Alarm	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		
Doctor Web Dr.Web	95.21%	95.21%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
ESET NOD32 Antivirus	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
Fortinet FortiClient	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
Frisk F-PROT Antivirus	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
F-Secure Client Security	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		2
G DATA AntiVirus 2008	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		
Hauri ViRobot	99.50%	99.50%	98.42%	98.42%	94.49%	94.49%	94.96%	94.96%	65.00%	65.00%		
Ikarus Virus Utilities	99.84%	99.84%	99.80%	99.80%	95.67%	95.67%	72.85%	72.85%	71.30%	71.30%	6	
K7 Total Security	99.93%	99.93%	99.53%	99.53%	97.32%	97.32%	59.45%	59.45%	77.91%	77.91%	2	2
Kaspersky Anti-Virus	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		
Kingsoft Internet Security 2008	100.00%	100.00%	35.00%	35.00%	75.00%	75.00%	48.00%	48.00%	56.00%	56.00%		
McAfee VirusScan Enterprise	99.998%	99.998%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
Microsoft Forefront Client Security	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	95.00%	95.00%	99.99%	99.99%		
Microsoft Windows Live OneCare	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	95.00%	95.00%	99.99%	99.99%		
MWTI eScan Internet Security	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		
Norman Virus Control	100.00%	100.00%	100.00%	100.00%	99.05%	98.43%	73.77%	70.23%	98.95%	98.95%	1	
PC Tools AntiVirus	99.99%	99.99%	100.00%	100.00%	99.21%	99.21%	79.29%	79.29%	99.98%	99.98%		2
Quick Heal Anti-Virus Lite	100.00%	100.00%	100.00%	100.00%	98.43%	98.03%	83.86%	83.86%	96.40%	96.40%	2	
Redstone Redprotect	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.88%	99.88%	100.00%	100.00%		
Rising Antivirus	99.97%	99.97%	99.73%	99.73%	93.70%	93.70%	44.63%	44.63%	56.40%	56.40%	1	
Security Coverage PC Live	84.35%	76.00%	56.00%	53.00%	97.20%	93.51%	54.00%	49.00%	47.00%	43.00%	1	
Sophos Anti-Virus	99.997%	99.997%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.80%	99.80%		
Symantec Norton AntiVirus	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%		
Trend Micro Internet Security	99.99%	99.99%	100.00%	100.00%	99.21%	99.21%	80.41%	80.41%	98.85%	98.04%	2	
VirusBuster Professional	99.99%	99.99%	100.00%	100.00%	99.21%	99.21%	79.29%	79.29%	99.98%	99.98%		2
Webroot Spy Sweeper with Antivirus	99.997%	99.997%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	99.98%	99.98%		

looked likely to be a tough month for the large crowd of products I dragged into the *VB* test lab.

AEC Trustport Antivirus 2.8.0.3001

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	97.62%
File infector	100.00%	**Polymorphic**	86.39%
False positives	0		

After a lengthy spell atop the scoreboard with near immaculate detection rates thanks to an intensive multi-engine design, *Trustport*'s performance dipped a little in recent tests which coincided with the product having a new set of engines under its bonnet. The version provided for this test was different again, with only the *Norman* and *AVG* engines in use this time. The look and feel of the product also seemed a little different, with the interface laid out in a pleasant and logical fashion, with access to the full range of configurations users of such a serious product should expect. The installation process was straightforward, requiring the administrator password and a reboot to complete.

In default mode, the 'intensive' settings option was selected, with all files and most archive types checked in both modes. As a result, scanning speeds were less than stellar and on-access overheads were on the high side. However, the product remained stable even under heavy bombardment and the system remained responsive throughout. Detection rates were solid, and with the WildList covered without problems *Trustport* regains its VB100 certified status.

Agnitum Outpost Security Suite Pro 6.0.2282.253.0485

ItW	99.99%	**Worms & bots**	100.00%
ItW (o/a)	99.99%	**Legacy**	99.98%
File infector	99.21%	**Polymorphic**	79.29%
False positives	0		

Agnitum's suite features a diverse set of security functions, and under *Vista* the installer requires both the administrator password and confirmation that the user does indeed want to install the software. After the obligatory reboot a message alerted me that a driver had failed to load, warning that functionality may be impaired, and the on-access scanner did seem to be working erratically. After a second reboot the error and related instability disappeared and all seemed to operate properly.

With a colourful and easy-to-use interface and a decent selection of options, testing proved a pleasure. Reporting was a little odd at times though, not least in the set where the Eicar test file was used to measure the depth of archive scanning – while in most types of archive the test file was described as 'malware', when stored in .tgz format it was labelled a virus and given a higher risk rating. This minor quibble aside, detection was pretty good throughout, with a few suspect packed files pointed out in the clean sets but no false positives. In the WildList set, however, a handful of samples from one of the newly expanded W32/Virut sets were missed, denying *Agnitum* a VB100 award this time.

Ahnlab V3 Internet Security 7.0 Platinum Enterprise

ItW	100.00%	**Worms & bots**	99.76%
ItW (o/a)	99.90%	**Legacy**	96.77%
File infector	99.21%	**Polymorphic**	88.06%
False positives	0		

Ahnlab's latest suite is a good-looking beast – glossy without being flashy – and installs simply, with the administrator password required but no reboot necessary. The main interface is similarly straightforward, offering some basic configuration – enough at least to get through the *VB* testing process without difficulty.

Logging seemed a little odd until I realised it had a hard-coded size limit for the log file, which meant that large chunks of precious detection records were being discarded before they could be saved. A somewhat laborious process of splitting the test sets up into several smaller chunks and scanning each separately got around this problem.

The product showed fairly good detection rates. A smattering of misses were recorded on access in the WildList set, thanks to some file extensions which are not scanned by default but are used by some worm variants for spreading. Thus, despite achieving full detection in manual scans and managing to avoid false positives across the expanded clean sets, *Ahnlab* does not reach the required standard for a VB100 award on this occasion.

Alwil avast! 4.7.1098

ItW	99.83%	**Worms & bots**	100.00%
ItW (o/a)	99.83%	**Legacy**	97.02%
File infector	100.00%	**Polymorphic**	86.20%
False positives	1		

Alwil's submission was troubled by some missing data, the problem being given away by the product running suspiciously quickly through the on-access tests. Once the correct files were in place, after an installation process which required no password for the normal user but did insist on a reboot, quite the opposite result was obtained. Speeds remained excellent over the clean sets but slowed right down when faced with large numbers of infected files. The entire system became bogged down in the process, and after leaving it to finish overnight another reboot was needed to pull itself together. Some investigation hinted that this was perhaps a result of the product deleting each infected file without prompting, despite the 'interactive' setting being selected. On demand things were less troublesome, with the action dialog appearing as usual with its friendly 'apply to all' option, and these scans sped through at a lightning pace.

The dual interface system has never been a favourite of mine, but here it seemed steady and responsive except during the on-access incident mentioned above, which does not reflect any likely real-world situation. Settings seemed plentiful, with defaults ignoring archives but full scanning available for those who want it, and detection rates were reasonable as ever. However, a set of file infectors recently added to the WildList set were missed, and a single item in the clean set was mistakenly flagged as malware, and thus *Alwil* misses out on a VB100 by a whisker.

AVG 7.5.516

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	97.63%
File infector	98.43%	**Polymorphic**	73.89%
False positives	0		

vb April 2008 100 VIRUS virusbtn.com

AVG (formerly known as *Grisoft*) provided the shiny new version of its product for a recent standalone review (see *VB*, March 2008, p.18), and it was with some disappointment that the earlier incarnation was received for this month's test, the new interface having impressed me considerably. This one required the administrator password to install as well as when changing settings, which seemed a sensible way to go about things. The available configuration, once I had managed to refamiliarise myself with its somewhat arcane layout, appeared to offer the option to scan all file types on access. However, this did not seem to cover archives, or even files with unusual extensions, which remained resolutely undetected. The settings also seemed to revert after a reboot, and having shut down the system over a long weekend I found, much to my annoyance, that the same scan I had run previously was now eating up my test collection.

Perhaps aided by the fact that it ignored many file types, speeds were excellent, and detection rates were also pretty good. With nothing missed in the Wild and no false positives, *AVG* earns its first VB100 award under its new company name.

Avira AntiVir Windows Workstation 7.06.00.507

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

Avira's *AntiVir* is another product that is familiar from many previous tests, this one offering a much more rational interface and a great flexibility of configuration. Defaults seemed sensible and increasing the range of items scanned produced impressively thorough results, without adding greatly to the excellent speeds.

Detection was similarly splendid, with not much missed across all the sets on demand. A strange anomaly on access left large swathes of the legacy set not spotted, but the items were detected without problems on demand and the oddity did not extend to the new sets. The WildList was fully covered and no false positives were generated in the clean sets, thus *Avira* wins another VB100 award.

BitDefender AntiVirus 2008

ItW	99.996%	**Worms & bots**	100.00%
ItW (o/a)	99.996%	**Legacy**	99.59%
File infector	98.95%	**Polymorphic**	100.00%
False positives	0		

BitDefender's 2008 product is another that has been subjected to an in-depth review in *VB* (see *VB*, September 2007, p.17) as well as repeated entries in *VB* comparative reviews, and thus proved familiar and simple to use. The interface achieves a happy balance between friendly straightforwardness for the less advanced user, displaying large and comforting green ticks and assurances that the system is protected, and in-depth configuration for those with more individual requirements.

Zipping through the speed tests in good time and getting near-perfect scores in the infected sets, it was only a pair of samples from the expanded set of W32/Virut variants that stood between *BitDefender* and a VB100 award.

Bullguard 8.0

ItW	99.996%	**Worms & bots**	100.00%
ItW (o/a)	99.996%	**Legacy**	99.59%
File infector	98.95%	**Polymorphic**	100.00%
False positives	0		

Bullguard requires the administrator password and a reboot before presenting its colourful interface and friendly 'Welcome to your Bullguard' sense of security. The version submitted for testing was presumably a trial version without a licence provided, and trying to run an on-demand scan brought up another demand for the admin password followed by the sad announcement that the scan could not continue as the licence had expired. Tests were able to proceed however, thanks to a right-click scanning option which mercifully remained functional.

With more thorough defaults on access than *BitDefender*'s own implementation of the same engine, speeds were pretty similar and detection levels likewise highly impressive with little missed in any of the sets. With no false positives only the two missed polymorphic samples in the WildList set prevented *Bullguard* earning itself another VB100 award.

CA eTrust Antivirus 8.1.637.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	99.10%
File infector	99.84%	**Polymorphic**	99.70%
False positives	0		

CA's corporate product remains unchanged once again, presenting the same interface for yet another test despite a few minor changes behind the scenes. The installation went through the traditional run of lengthy EULAs, personal data gathering and complex activation codes, but with the benefit of much experience the product was quickly up and running.

Experience is of little help once the fiddly and frustratingly slow-to-respond interface comes into play, but the tests proceeded despite a lack of available configuration, and at the usual excellent speed. Although the interface appeared to provide the option to scan inside archives there was no evidence of this actually happening.

Logging was awkward, and trying to view logs of any significant size from within the product brought about a grinding freeze. As usual the logs were taken off the system and converted into normal text, dropping much of their extraneous content, for parsing. Results showed an absence of false positives and pretty decent detection, and with nothing missed in the WildList *eTrust* adds another VB100 award to its tally.

CA Internet Security 4.0.0.172

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	99.10%
File infector	99.84%	**Polymorphic**	99.70%
False positives	0		

CA's home-user product also eschews the admin password and simply requires a 'continue' button to be clicked to install, as well as each time the configuration is changed. This was not often though, as little configuration was available, and again archives could not be scanned internally on access; speeds were extremely impressive.

Detection also kept up with the corporate product, and false positives were absent again. After several detections in a small test scan, identical alert popups appeared repeatedly – over a dozen times for a single detection – but this behaviour did not recur, thankfully, while scanning the full test sets. With nothing missed in the wild and no false positives, *CA* notches up its second award of the month.

Check Point Zone Alarm

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

Since I joined *VB* some time ago, *Zone Alarm* has been one of the highest-profile products not to appear in our tests. Frequent queries from readers have diligently been followed up with attempts to contact the vendor, and at last the good people at *Check Point* have seen fit to submit a product for testing. I installed it with excitement.

The installation process was a little complex, thanks to the test lab being isolated from the web to ensure all products are tested on a level field. Once the installer had been run, using the admin password, and detection data had been replaced in safe mode, the product finally presented an interface that was little changed from the one I had grown accustomed to many years ago when running the free version of the firewall on a home system. In the modern setting of *Windows Vista* (even without the fancy Aero stylings), it looks a little dated and perhaps in need of a restyle, but there's much to be said for sticking with the tried and trusted.

The suite includes intrusion prevention, email filtering and spyware monitoring as well as the anti-virus and firewall, and little room has been left in the interface for in-depth configuration of the virus scanning. There was, however, enough control to get through our tests, and detection, provided by the *Kaspersky* engine, was as excellent as one would expect.

Scanning times were somewhat slow on demand, quite spectacularly so over the archive set, but not unacceptable on access, and the product seemed to run stably with no noticeable impact on system performance. With nothing missed in the WildList set, and precious little elsewhere, and nothing more than a few warnings of possibly unwanted items in the clean set, *Check Point*'s product wins itself its first VB100 award at the first attempt, without even breaking into a sweat.

Doctor Web Dr.Web 4.44.4

ItW	95.21%	**Worms & bots**	100.00%
ItW (o/a)	95.21%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	100.00%
False positives	0		

Doctor Web's product requires its installer to be run with full administrator rights, and requires the password again for updating and changing settings. The product is split into two quite separate parts, the scanner and the on-access component, 'SpIDer Guard'. The latter seemed to be having some difficulties operating on this occasion, but disabling *Windows Defender*, the security tool which runs by default under *Vista*, put an end to this problem.

Scanning was thorough rather than speedy, with thoroughness particularly evident on the archive sets. Detection rates were as good as ever, and false positives absent, but once again a handful of the latest additions to the WildList set were not detected, and *Doctor Web* misses out on a VB100 award.

ESET NOD32 Antivirus 3.0.642.0

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

The recent overhaul of *ESET*'s product, both cosmetically and at a deeper level, has added considerably to *NOD32*'s charms. The installation was one of the most straightforward, with a simple 'continue' prompt and no reboot, and with ample configuration and typically zippy scanning speeds, testing took barely any time at all.

Detection was as flawless as usual, with nothing missed across any of the sets, and *ESET* continues its lengthy run of success with another VB100 award.

Fortinet FortiClient Host Security 3.0.470

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

FortiClient has a rather more complex installation process thanks to its multi-function nature, and requires confirmation of numerous drivers as the process chugs along. Once it is installed, much of the configuration is greyed out for the normal user and requires the interface be opened with the 'Run as administrator' option to allow the settings to be changed, although no password is required to access this.

Considering the thoroughness of the scanning, speeds were surprisingly good. At the end of one large scan the product froze and had to be shut down forcibly, but this was the only significant problem encountered – detection was splendid, false positives absent, and *Fortinet* wins itself another VB100 award.

Frisk F-PROT Antivirus for Windows 6.0.8.1

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

The version of *F-PROT* submitted for testing described itself as a beta version and advised would-be users only to install it on test systems. This didn't put me off, and I proceeded merrily with the install, pausing only to enter the administrator password. The interface presented is a simple, pared-down little thing, not heavy on the configuration options, but it runs solidly and smoothly. My only quibble with it would be that the scanning page seems to snag in one place after scans, and must be clicked away from and back to in order to access the controls again.

Speeds were splendid and detection excellent, and with no significant misses in the infected sets and no false positives, *Frisk* qualifies for a VB100 award this month.

F-Secure Client Security 7.11.107

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

F-Secure's installation process has the full range of requirements – passwords, licence codes, a reboot, and admin rights are required to run the offline update. It even seems to limit the configuration controls for less privileged users, and it offers the option of installing a standalone or remotely managed version from the off.

Scanning seemed fairly fast, at least until more thorough options are selected, but there did seem to be some noticeable slowing of the system. This impact was made up for by the superb detection which, coupled with a lack of false positives earns *F-Secure* a VB100 award once again.

G DATA AntiVirus 2008 18.4.8051.821

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

G DATA seems to have dropped the cosy 'AVK' from its latest product names, but little else has changed in this multi-engine powerhouse. Installation needed no password, but a 'continue' prompt appeared during the install as well as each time the options page was visited and whenever a manual scan was initiated. After the install, the product requested a reboot, but with the prompt hidden behind another window it wasn't noticed for some time; this didn't seem to affect the running of the product in any way, however, and testing progressed with much success before it was spotted.

The interface is attractive and well designed, with none of my specialist requirements absent or hard to find. Logging, however, has long posed a problem, with details spread over multiple lines requiring some extra tinkering to extract data. This time the headache was increased by the log file taking a long time to open. Once acquired and processed however, detection proved to have been almost impeccable, and with nothing missed in the wild and no false positives *G DATA* once again qualifies for a VB100 award.

Hauri ViRobot Desktop 5.5

ItW	99.50%	**Worms & bots**	98.42%
ItW (o/a)	99.50%	**Legacy**	65.00%
File infector	94.49%	**Polymorphic**	94.96%
False positives	0		

Hauri has been absent from the *VB* test bench for some time, its last appearance also being the last test conducted by my predecessor (see *VB*, June 2006, p.11). After this lengthy break the *ViRobot* product returns to the fold, bravely, just in time for one of the toughest tests for a while.

The installation, which required no password, mentioned that some technology provided by *BitDefender* was included in the product – which promised good things. The interface looked well designed and ran in a solid and stable manner; configuration was ample and well presented. One option which was conspicuously absent was a control to deactivate the beep made each time a detection is recorded on access – I had to flee the lab to escape the barrage of sounds as the full test set flooded past the scanner.

Archive detection seemed sensible, with no scanning on access and a maximum of five levels on demand, and speeds were comfortably in the mid-range. Logging took an enormous amount of time to deal with. Saving the log file left me gazing forlornly at an egg timer for ages only for a log to be produced in the most bizarre format I have ever encountered, and one which required considerable hacking to render it readable. Scanning results revealed an absence of false positives, but several misses in the WildList set and less than perfect coverage elsewhere. Consequently, *Hauri* does not quite reach the required standard for a VB100 award this time.

Ikarus Virus Utilities 1.0.61

ItW	99.84%	**Worms & bots**	99.80%
ItW (o/a)	99.84%	**Legacy**	71.30%
File infector	95.67%	**Polymorphic**	72.85%
False positives	6		

Plucky *Ikarus* continues to fling itself at the walls of the VB100 fortress, despite repeated knock-backs in recent tests. Each time the product has seemed to improve in stability and detection rates, but this trend slowed somewhat this month. After a solid start, with some sensible integration into the UAC system requiring administrative rights to install and alter settings, the interface seemed reluctant to open over several attempts, and once running provided the usual dearth of options.

The .NET-based GUI also suffered some shakiness during scanning, with flickering and ghostly whiting out not uncommon, especially when scanning large sets. A limitation on the size of logs meant on-demand scans had to be carried out in smaller chunks, and once all the information presented was processed the results showed several file-infecting viruses not fully covered in the WildList set. With a smattering of false positives as well, *Ikarus*' quest for VB100 certification must continue another day.

K7 Total Security 9.5.0502

ItW	99.93%	**Worms & bots**	99.53%
ItW (o/a)	99.93%	**Legacy**	77.91%
File infector	97.32%	**Polymorphic**	59.45%
False positives	2		

K7 achieved VB100 certification at its first attempt a little under a year ago, but then disappeared from our radar for some time, missing out on several less arduous tests only to return in time for a tricky platform. The product handled the new surroundings with some ease however, requiring the admin password and a reboot to get running, and asking for a username and email address to keep in touch with users, before presenting a clear and stable interface.

UAC was again integrated with the product, with on-access controls disabled for unprivileged users, although oddly anyone has the power to disable on-access scanning completely. Scanning speeds were excellent and though configuration was not available in any great depth the defaults seemed sensibly chosen. Detection was no more than reasonable across the sets, however, with a handful of tricky polymorphic items missed in the WildList set and a clutch of false positives in the clean set spoiling *K7*'s immaculate VB100 record.

Kaspersky Anti-Virus 7.0.1.325

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

Kaspersky has a much longer and more illustrious record, producing consistently excellent detection rates and unimpeachable standards of design and implementation. As usual the product proved thorough rather than speedy, but still produced perfectly acceptable times even over archive sets, and powered through the infected sets with little difficulty.

With nothing missed in the WildList and no false positives, *Kaspersky* easily wins another award for its collection.

Kingsoft Internet Security 2008.2.22.11

ItW	100.00%	**Worms & bots**	35.00%
ItW (o/a)	100.00%	**Legacy**	56.00%
File infector	75.00%	**Polymorphic**	48.00%
False positives	0		

Kingsoft has a single VB100 award under its belt, gained in last year's 64-bit *Vista* test. The product has shown some decent detection levels in the newer sets, and presents a slick and professional-looking interface, but has on occasion been a little inconsistent in its scanning behaviour.

This was another of those occasions, with an initial install seeming to miss well over half the samples in most sets. Assuming there were some problems, the installation was re-run with full admin rights (a password had been required as a normal user) and things seemed to go somewhat more smoothly. After several re-runs and re-scans, the product managed to squeeze out some reliable results, with the WildList samples covered in full but a surprising number of misses still evident in the set of worms, many of which have been detected by the product in the past. Nevertheless, *Kingsoft* scrapes its way to a second VB100 award.

McAfee VirusScan Enterprise 8.5.0i

ItW	99.998%	**Worms & bots**	100.00%
ItW (o/a)	99.998%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	100.00%
False positives	0		

McAfee is another old-timer with a long history of success in VB100 testing. The product remains little changed and its simple, dependable style always makes it a welcome visitor to the test lab. The UAC integration is solid, as one would expect from an enterprise-class product, with passwords required to install and on-access controls pared down for non-administrative users.

Everything ran solidly and well with no difficulties caused by the new platform. Speeds were decent and detection rates dependably excellent, until another single sample of the W32/Virut strain which has caused a few upsets already this month reared its ugly head, and since it was in the WildList set was enough to deny *McAfee* a VB100 award this time.

Microsoft Forefront Client Security 1.5.1937.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	99.99%
File infector	100.00%	**Polymorphic**	95.00%
False positives	0		

Another giant company, *Microsoft* provides two anti-malware products that ooze professional attention to detail and solidity, and should have been well tested on the new service pack for *Vista*. Both products contrast starkly with the previous offerings however, in their minimal flexibility. Configuration is barely present – the few choices that are available require the administrator password to access them.

Logging is another area which is kept to a minimum. An uncooperative 'History' page lingered regularly for long periods before opening and often showed no detections despite having recently scanned large infected test sets. All data had to be extracted, with some difficulty, from the *Windows* event log, but when finally checked over it showed detection was very good. With the WildList fully covered *Forefront* qualifies for a VB100 award.

Microsoft Windows Live OneCare 2.0.2500.22

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	99.99%
File infector	100.00%	**Polymorphic**	95.00%
False positives	0		

On Demand Throughput (MB/S)	Archive Files				Binaries and System Files				Media and Documents				Other File Types			
	Default Settings		All Files		Default Settings		All Files		Default Settings		All Files		Default Settings		All Files	
	Time	Through-put	Time	Through-put	Time	Through-put	Time	Through-put	Time	Through-put	Time	Through-put	Time	Through-put	Time	Through-put
AEC Trustport Antivirus	1258	3.1	1258	3.1	639	6.1	639	6.1	147	12.2	147	12.2	220	4.2	220	4.2
Agnitum Outpost Security Suite Pro	1777	2.2	1777	2.2	448	8.7	448	8.7	122	14.7	122	14.7	100	9.3	100	9.3
Ahnlab V3	1350	2.9	1350	2.9	606	6.4	606	6.4	82	21.8	82	21.8	144	6.4	144	6.4
Alwil avast!	32	123.8	1066	3.7	325	11.9	335	11.6	39	45.9	96	18.7	33	28.0	74	12.5
AVG	1828	2.2	1828	2.2	576	6.7	576	6.7	97	18.5	97	18.5	125	7.4	125	7.4
Avira AntiVir	920	4.3	920	4.3	142	27.3	142	27.3	45	39.8	45	39.8	32	28.9	32	28.9
BitDefender AntiVirus 2008	1506	2.6	1506	2.6	526	7.4	526	7.4	89	20.1	89	20.1	95	9.7	95	9.7
Bullguard	1967	2.0	1967	2.0	560	6.9	560	6.9	99	18.1	99	18.1	112	8.3	112	8.3
CA eTrust Antivirus	841	4.7	841	4.7	103	37.6	103	37.6	46	38.9	46	38.9	38	24.3	38	24.3
CA Internet Security	1257	3.2	N/A	N/A	130	29.8	130	29.8	53	33.8	53	33.8	44	21.0	44	21.0
Check Point Zone Alarm	12271	0.3	12271	0.3	308	12.6	308	12.6	598	3.0	598	3.0	657	1.4	657	1.4
Doctor Web Dr.Web	5226	0.8	5226	0.8	210	18.5	210	18.5	169	10.6	169	10.6	181	5.1	181	5.1
ESET NOD32 Antivirus	1322	3.0	1322	3.0	801	4.8	801	4.8	42	42.7	42	42.7	59	15.7	59	15.7
Fortinet FortiClient	561	7.1	561	7.1	708	5.5	708	5.5	39	45.9	39	45.9	71	13.0	71	13.0
Frisk F-PROT Antivirus	287	13.8	287	13.8	455	8.5	455	8.5	43	41.7	43	41.7	36	25.7	36	25.7
F-Secure Client Security	3192	1.2	3362	1.2	342	11.3	340	11.4	49	36.6	110	16.3	33	28.0	126	7.3
G DATA AntiVirus 2008	2947	1.3	3416	1.2	543	7.1	544	7.1	133	13.5	160	11.2	123	7.5	133	7.0
Hauri ViRobot	811	4.9	811	4.9	735	5.3	735	5.3	103	17.4	103	17.4	131	7.1	131	7.1
Ikarus Virus Utilities	186	21.3	N/A	N/A	436	8.9	436	8.9	66	27.1	66	27.1	116	8.0	116	8.0
K7 Total Security	276	14.4	N/A	N/A	185	21.0	185	21.0	30	59.7	30	59.7	30	30.8	30	30.8
Kaspersky Anti-Virus	2658	1.5	2658	1.5	613	6.3	613	6.3	115	15.6	115	15.6	122	7.6	122	7.6
Kingsoft Internet Security 2008	465	8.5	465	8.5	735	5.3	735	5.3	37	48.4	37	48.4	61	15.2	61	15.2
McAfee VirusScan Enterprise	60	66.0	988	4.0	493	7.9	494	7.8	87	20.6	86	20.8	102	9.1	110	8.4
Microsoft Forefront Client Security	1469	2.7	1469	2.7	867	4.5	867	4.5	78	23.0	78	23.0	69	13.4	69	13.4
Microsoft Windows Live OneCare	1247	3.2	1247	3.2	658	5.9	658	5.9	107	16.7	107	16.7	74	12.5	74	12.5
MWTI eScan Internet Security	2683	1.5	2683	1.5	637	6.1	637	6.1	468	3.8	468	3.8	472	2.0	472	2.0
Norman Virus Control	999	4.0	999	4.0	2120	1.8	2120	1.8	81	22.1	81	22.1	231	4.0	231	4.0
PC Tools AntiVirus	683	5.8	963	4.1	355	10.9	357	10.9	77	23.3	77	23.3	77	12.0	77	12.0
Quick Heal Anti-Virus Lite	1133	3.5	1217	3.3	94	41.3	95	40.8	77	23.3	83	21.6	57	16.2	73	12.7
Redstone Redprotect	2089	1.9	2089	1.9	554	7.0	554	7.0	274	6.5	274	6.5	273	3.4	273	3.4
Rising Antivirus	2359	1.7	2359	1.7	1158	3.3	1158	3.3	278	6.4	278	6.4	138	6.7	138	6.7
Security Coverage PC Live	[8000+]	[>0.5]	[8000+]	[>0.5]	1074	3.6	1074	3.6	[3600+]	[>0.5]	[3600+]	[>0.5]	130	7.1	130	7.1
Sophos Anti-Virus	51	77.7	2166	1.8	376	10.3	411	9.4	71	25.2	95	18.9	137	6.8	129	7.2
Symantec Norton AntiVirus	406	9.8	406	9.8	562	6.9	562	6.9	165	10.9	165	10.9	146	6.3	146	6.3
Trend Micro Internet Security	527	7.5	661	6.0	316	12.3	319	12.2	94	19.1	94	19.1	103	9.0	103	9.0
VirusBuster Professional	598	6.6	1265	3.1	353	11.0	384	10.1	33	54.3	69	26.0	22	42.1	68	13.6
Webroot Spy Sweeper with Antivirus	1109	3.6	1109	3.6	504	7.7	504	7.7	61	29.4	61	29.4	61	15.2	61	15.2

Like its big brother *Forefront*, *Microsoft*'s home-user product looks slick and smooth, integrates sensibly with the user access controls and offers precious little by way of configuration options. Its insistent pestering to be allowed to disinfect items, and habit of scanning 'additional locations' after a scan of a selected area (for several hours in one instance) slowed testing down somewhat, but actual speeds were quite good and detection once again impressive.

Sharing technology and detection data with *Forefront*, it was no surprise to see *OneCare* achieving similarly high detection rates, covering the WildList in full including the tricky sets of polymorphic samples, and joining its stablemate on the VB100 award podium.

MWTI eScan Internet Security 9.0.779.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

Microworld's implementation of the *Kaspersky* scanning engine has numerous additional bells and whistles, and requires several extras be installed including some C++ components and, rather unexpectedly, an update from the *Microsoft* knowledgebase. All of these are thoughtfully provided and only need confirmation to proceed. A management console for multiple installs is also offered.

Once up and running, the product provides an excellent interface with all the controls one could ever need. Default settings are turned up to the max and scanning was a little languid but results impeccable. With excellent detection throughout, and no false positives, *eScan* earns yet another VB100 award.

Norman Virus Control 5.90

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	98.95%
File infector	99.05%	**Polymorphic**	73.77%
False positives	1		

Norman once again required the admin password to get started but after that provided a very speedy and simple installation, with just four or five hits on the enter key, the offer of an update (which was declined), and a few seconds pause before everything was up and running. A rather bizarre error message suggesting I had no hard drives appeared briefly but seemed to have no impact on functionality, and tests plodded along merrily.

Scanning options were somewhat limited, but a range of common archive types were scanned by default on demand, adding considerably to the scanning time over the archive set. Other scans were mostly pretty speedy, but the set of clean executables took rather a long time on demand. Detection was at its usual high level, with no problems posed by the W32/Virut sets, although somewhat annoyingly the samples were deleted or disinfected despite specifying explicitly the ‘please-don’t-destroy-my-test-set’ option. In the clean sets a single item was mislabelled as malware, leaving *Norman* a fraction short of the required standard for VB100 certification.

PC Tools AntiVirus 2008 4.0.0.25

ItW	99.99%	**Worms & bots**	100.00%
ItW (o/a)	99.99%	**Legacy**	99.98%
File infector	99.21%	**Polymorphic**	79.29%
False positives	0		

The *PC Tools* product evolved from the company’s anti-spyware speciality and closely resembles its *Spyware Doctor* flagship offering. This version has a few tweaks which provide an experience pretty similar to any other anti-virus product aimed squarely at the home-user market: bright and colourful, with simple controls and limited configuration. The installer offered to include a toolbar from *Google*, which I declined, but was otherwise fairly straightforward.

Adjustments made by the developers to the default settings caused some early difficulties when it was found that the on-access scanning is now in most cases only activated when fully executing files. Viewing the files in *Explorer* also sparked some detection, but with large numbers of folders needing checking it was felt simplest to adjust the setting to scan files when opened via the testing script. The option to provide this seemed not to function at first, but after a reinstallation everything was fine and testing continued without too much trouble.

The system was a little unresponsive at times, and after scanning the full collection the product interface – along with the rest of the screen – got rather snarled up and couldn’t be used until after a reboot. Eventually results were gathered showing good detection and decent speeds, but as with other products based on the *VirusBuster* engine, a few of those nasty Virut samples were missed in the WildList set and a VB100 award is just out of reach for *PC Tools* this month.

Quick Heal Anti-Virus Lite 9.50

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	96.40%
File infector	98.43%	**Polymorphic**	83.86%
False positives	2		

Quick Heal was listed in my submission set under the company’s former name, *CAT*, and thus was run rather early on in the test prior to the many frustrations and annoyances which built up in the second half of the product set. It fitted better here anyway, providing amply for my needs with a simple, flexible and highly stable product.

Scanning proceeded at tip-top speeds, with the product’s usual decent level of detection and only the older items bringing the scores below excellent. The WildList was ably covered despite the many tricky items, but in the clean set yet more false positives appeared, spoiling *Quick Heal’s* chance of a VB100 for a second time in a row.

Redstone Redprotect 0.5.3.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**Legacy**	100.00%
File infector	100.00%	**Polymorphic**	99.88%
False positives	0		

Redprotect is still a relatively young product with a little development to go before it settles into full stability. The

File Access Lag time (S/MB)	Archive Files				Binaries and System Files				Media and Documents				Other File Types			
	Default Settings		All Files		Default Settings		All Files		Default Settings		All Files		Default Settings		All Files	
	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag
AEC Trustport Antivirus	1259	0.32	1259	0.32	666	0.17	666	0.17	178	0.08	178	0.08	241	0.23	241	0.23
Agnitum Outpost Security Suite Pro	79	0.02	N/A	N/A	583	0.14	583	0.14	231	0.11	231	0.11	219	0.21	219	0.21
Ahnlab V3	136	0.03	N/A	N/A	674	0.17	N/A	N/A	101	0.04	N/A	N/A	86	0.06	N/A	N/A
Alwil avast!	102	0.02	1080	0.27	343	0.08	430	0.10	174	0.08	207	0.10	88	0.07	93	0.07
AVG	29	0.01	N/A	N/A	208	0.05	212	0.05	52	0.01	60	0.02	41	0.02	71	0.05
Avira AntiVir	37	0.01	108	0.03	149	0.03	178	0.04	64	0.02	82	0.03	40	0.01	80	0.06
BitDefender AntiVirus 2008	331	0.08	775	0.19	532	0.13	562	0.14	114	0.05	225	0.11	124	0.10	129	0.11
Bullguard	1098	0.28	1098	0.28	568	0.14	568	0.14	104	0.04	104	0.04	117	0.10	117	0.10
CA eTrust Antivirus	26	0.01	N/A	N/A	119	0.02	119	0.02	72	0.02	72	0.02	68	0.04	68	0.04
CA Internet Security	32	0.01	N/A	N/A	139	0.03	139	0.03	79	0.03	79	0.03	69	0.05	69	0.05
Check Point Zone Alarm	61	0.01	N/A	N/A	322	0.08	322	0.08	141	0.06	141	0.06	134	0.12	134	0.12
Doctor Web Dr.Web	760	0.19	4705	1.19	748	0.19	1074	0.27	162	0.07	209	0.10	161	0.14	230	0.22
ESET NOD32 Antivirus	14	0.00	N/A	N/A	86	0.02	86	0.02	72	0.02	72	0.02	80	0.06	80	0.06
Fortinet FortiClient	429	0.11	429	0.11	728	0.18	728	0.18	55	0.02	55	0.02	95	0.07	95	0.07
Frisk F-PROT Antivirus	83	0.02	N/A	N/A	484	0.12	484	0.12	67	0.02	67	0.02	57	0.03	57	0.03
F-Secure Client Security	54	0.01	2096	0.53	349	0.08	609	0.15	84	0.03	249	0.12	58	0.03	202	0.19
G DATA AntiVirus 2008	293	0.07	862	0.22	518	0.13	541	0.13	241	0.12	252	0.12	175	0.16	181	0.17
Hauri ViRobot	256	0.06	N/A	N/A	536	0.13	536	0.13	107	0.04	107	0.04	117	0.10	117	0.10
Ikarus Virus Utilities	192	0.05	215	0.05	456	0.11	747	0.19	91	0.04	99	0.04	138	0.12	139	0.12
K7 Total Security	66	0.02	N/A	N/A	221	0.05	221	0.05	63	0.02	63	0.02	67	0.04	67	0.04
Kaspersky Anti-Virus	18	0.00	171	0.04	110	0.02	294	0.07	114	0.05	143	0.06	82	0.06	132	0.11
Kingsoft Internet Security 2008	36	0.01	N/A	N/A	751	0.19	751	0.19	54	0.01	54	0.01	73	0.05	73	0.05
McAfee VirusScan Enterprise	55	0.01	808	0.20	509	0.12	499	0.12	92	0.04	93	0.04	97	0.08	97	0.08
Microsoft Forefront Client Security	127	0.03	N/A	N/A	589	0.15	589	0.15	95	0.04	95	0.04	86	0.06	86	0.06
Microsoft Windows Live OneCare	149	0.04	N/A	N/A	596	0.15	596	0.15	96	0.04	96	0.04	94	0.07	94	0.07
MWTI eScan Internet Security	1413	0.36	1413	0.36	394	0.10	394	0.10	166	0.08	166	0.08	160	0.14	160	0.14
Norman Virus Control	40	0.01	N/A	N/A	365	0.09	365	0.09	104	0.04	104	0.04	150	0.13	150	0.13
PC Tools AntiVirus	5	0.00	N/A	N/A	189	0.04	189	0.04	209	0.10	209	0.10	160	0.14	160	0.14
Quick Heal Anti-Virus Lite	16	0.00	N/A	N/A	102	0.02	102	0.02	69	0.02	69	0.02	39	0.01	39	0.01
Redstone Redprotect	70	0.02	N/A	N/A	387	0.09	387	0.09	209	0.10	209	0.10	203	0.19	203	0.19
Rising Antivirus	92	0.02	419	0.10	645	0.16	696	0.17	160	0.07	161	0.07	176	0.16	179	0.16
Security Coverage PC Live	232	0.06	232	0.06	405	0.10	405	0.10	106	0.04	106	0.04	96	0.08	96	0.08
Sophos Anti-Virus	43	0.01	1391	0.35	383	0.09	412	0.10	68	0.02	88	0.03	68	0.04	117	0.10
Symantec Norton AntiVirus	30	0.01	N/A	N/A	254	0.06	254	0.06	73	0.02	73	0.02	67	0.04	67	0.04
Trend Micro Internet Security	84	0.02	610	0.15	298	0.07	290	0.07	74	0.03	105	0.04	82	0.06	93	0.07
VirusBuster Professional	36	0.01	N/A	N/A	375	0.09	375	0.09	59	0.02	90	0.03	44	0.02	89	0.07
Webroot Spy Sweeper with Antivirus	10	0.00	N/A	N/A	46	0.01	N/A	N/A	67	0.02	N/A	N/A	61	0.04	N/A	N/A

offering is part of a managed security setup intended to be controlled from a web interface supervising a large number of systems, but the developers thoughtfully provided a testing tool to access controls without having to delve into the registry (in a fully operational setup such changes made by the end-user would quickly be reverted to the master settings).

An initial run proved puzzlingly ineffective, until I remembered that the trial licence for the *Kaspersky* engine powering the product was set to expire halfway through the test period. The addition of an updated key file quickly had things moving along nicely. Although limitations to the settings meant the test collection had to be deleted on access, things still moved along at a pleasingly rapid pace with no major hiccups. The .NET-based interface presented the flakiness I have come to expect from such things, occasionally failing to open or to run a scan when requested, but generally responding well. Results reflected the solid engine at the heart of things, with splendid detection and no false positives earning *Redstone* another VB100 award.

Rising Antivirus 20.33.10

ItW	99.97%	**Worms & bots**	99.73%
ItW (o/a)	99.97%	**Legacy**	56.40%
File infector	93.70%	**Polymorphic**	44.63%
False positives	1		

Beijing-based *Rising* had its first stab at the VB100 at the end of last year and missed out on certification by a whisker; it was good to see the company bravely back in the saddle. An initial attempt at installing the product went somewhat awry – after demanding the admin password, things seemed to be going well until after the requested reboot, when a message popped up insisting that another reboot was required. Switching to full admin user, I clicked on the desktop shortcut set up during the install, only to find an uninstallation process initiated. Bewildered, I switched to a fresh machine and tried installing with full administrative rights and the UAC controls disabled.

This time everything ran smoothly, eventually bringing up a nice shiny interface and a cute little cartoon lion which lurked in the corner of my desktop occasionally performing stunts, and whipping out a magnifying glass and peering around when scans were run.

The scans seemed to go smoothly too, at a fairly leisurely pace but with very thorough default settings on demand – the on-access controls offered an option to enable archive scanning which, although slowing things down a fraction, seemed to have no effect on detection rates. Disabling the on-access component brought up a CAPTCHA for confirmation, presumably to prevent infiltrations from switching it off.

Detection was fairly good on more recent items, but a small number of polymorphic items in the WildList set were missed and a single false positive was flagged in the clean set. As a result, *Rising* does not quite make it to a VB100 award this time.

Security Coverage PC Live

ItW	84.35%	**Worms & bots**	56.00%
ItW (o/a)	76.00%	**Legacy**	47.00%
File infector	97.20%	**Polymorphic**	54.00%
False positives	1		

PC Live marks the first appearance of the open-source *ClamAV* engine on the VB100 test bench, though it was not the only product based on this engine to be submitted (more on this later). Like many commercial products in the open-source world, *PC Live* is provided as a free tool funded by paid-for support, and the interface is bright and colourful, apparently aiming at the PC novice market with its 1950s soap powder stylings.

As a result, configuration is less than ideal for my requirements, with logging particularly awkward, but things seemed to run pretty smoothly and stability was not a problem. Scanning speeds were rather impressive on access, but less so on demand, with some of the scans of the clean sets abandoned after having been left to run longer than any of the rest of the field, hinting at some kind of snagging issue. Detection results were not excellent, with a pronounced difference between on-demand and on-access scores and with large numbers of clean files blocked on access with no explanation. This implies that the on-access side of things also needs a little improvement.

With the *ClamAV* technology now backed by a commercial firm this could well prove a contender for a VB100 award in the near future, but for now a number of WildList misses and a false positive deny *Security Coverage* its first VB100 award.

Sophos Anti-Virus 7.0.7

ItW	99.997%	**Worms & bots**	100.00%
ItW (o/a)	99.997%	**Legacy**	99.80%
File infector	100.00%	**Polymorphic**	100.00%
False positives	0		

Sophos is a much more familiar product, and another that has changed little for some time. It has a solid simplicity about it which has become an increasingly welcome sight on the test bench, providing respite from the strange and bewildering array of newcomers. Installing the product and opening the interface brings up a confirmation prompt but no password is needed.

As an enterprise-level product there is, of course, a full range of configuration options, making testing a breeze. Speeds were impressive, even with all files and archive types enabled on access, and detection was pretty good across the sets. Once again, however, a couple of samples of the trickiest of those Virut variants were not detected, and *Sophos* misses out on a VB100 award this month.

Symantec Norton Anti-Virus 15.5.0.23

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

Despite having tested a wide range of anti-malware products on a regular basis for some years, and despite *Symantec*'s *Norton AntiVirus* being one of the biggest and most widely used products on the market, this is the first time our paths have crossed in any serious fashion.

Initial impressions were not good, the product presenting a rather sickly look with its gaudy yellow on a background of shimmering black, and

Archive scanning		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
AEC Trustport Antivirus	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	X	√	√	√	√	√	√
Agnitum Outpost Security Suite Pro	OD	1	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Ahnlab V3 Internet Security	OD	X	9	X	9	9	X	9	X	√
	OA	X	X	X	X	X	X	X	X	X
Alwil avast!	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/8	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
AVG	OD	X	√	1	X	√	X	√	√	X
	OA	X	X	X	X	X	X	X	X	X
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	√*	√	√	√	√	√	√	√	√
BitDefender AntiVirus 2008	OD	√	√	√	√	√	8	√	8	√
	OA	X/√	X/√	√	X/√	X/√	X/8	1/√	X/8	√
Bullguard	OD	√	√	√	√	√	8	√	8	√
	OA	√	√	√	√	√	8	√	8	√
CA eTrust Antivirus	OD	X	√	√	√	√	√	√	X	√
	OA	X	X	1	X	X	X	1	X	√
CA Internet Security	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	X	√
Check Point Zone Alarm	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Doctor Web Dr.Web Antivirus	OD	X	√	√	√	√	X/4	X/9	X/8	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
ESET NOD32 Antivirus	OD	X	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	4	√	√
	OA	X	√	√	√	√	√	4	√	√
Frisk F-PROT Antivirus	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	2	X	X	X	2	2	√
F-Secure Client Security	OD	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
G DATA AntiVirus 2008	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	8	8	4	√
Hauri ViRobot Desktop	OD	5	5	5	5	5	5	5	5	√
	OA	X	X	X	X	X	X	X	X	√
Ikarus Virus Utilities	OD	2	3	3	3	3	1	3	1	√
	OA	2	3	3	3	3	1	3	1	√
K7 Total Security	OD	X	1	1	1	1	X	1	X	√
	OA	X	X	X	X	X	X	X	X	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/4	X/4	X/4	X/4	X/5	X/1	X/2	X/1	√
Kingsoft Internet Security 2008	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan Enterprise	OD	2/X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	2/X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Microsoft Forefront Client Security	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	1	√
Microsoft Windows Live OneCare	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	1	√
MWTI eScan Internet Security	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Virus Control	OD	X	X	√	√	X	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
PC Tools AntiVirus	OD	1/2	1/√	1/√	X	1/√	X/√	1/√	1/√	√
	OA	1	1	1	X	1	X	1	1	√
Quick Heal Anti-Virus Lite	OD	X/2	2/5	2/5	X	2/5	1	2/5	X	X/√
	OA	X	X	X	X	X	X	X	X	X
Redstone Redprotect	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Rising Antivirus	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Security Coverage Pc Live	OD	X	X	√	X	√	√	√	√	√
	OA	X	X	5	X	5	X	5	X	√
Sophos Anti-Virus	OD	X	5	5	5	5	5	5	5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Norton AntiVirus	OD	X	9	9	9	9	9	9	9	√
	OA	X	X	X	X	X	X	X	X	√
Trend Micro Internet Security	OD	3/6	3/6	3/6	3/6	3/6	1/3	3/6	X	√
	OA	X/6	X/6	X/6	X/6	X/6	1/3	X/6	X	√
VirusBuster Professional	OD	1	√	X/√	X	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot Spy Sweeper with Antivirus	OD	X	√	5	√	√	6	√	5	√
	OA	X	X	X	X	X	X	X	X	√

presenting a few error messages about the 'service framework' having stopped working as well as some nondescript internal errors.

In spite of this the product seemed to run pretty solidly with no problems in detection – this took some time to work out though, as the product defaults to removing or disinfecting items, with virtually no configuration options available to the user. This meant that on-access results had to be gathered by means of checking remaining files for changes, and the on-demand scan needed to be left overnight to complete its lengthy operations. It then needed to be re-run as I had missed the unobtrusive button needed to save the scanning log, which is not available from the history screen.

At the end of all this everything seemed okay, with splendid detection rates and no false positives. As a result, *Norton AntiVirus* gains a VB100 award, but does not make any new friends.

Trend Micro Internet Security 16.10.1063

ItW	99.99%	**Worms & bots**	100.00%
ItW (o/a)	99.99%	**Legacy**	98.85%
File infector	99.21%	**Polymorphic**	80.41%
False positives	2		

Trend Micro's product is another slick and professional piece of work from an industry giant, and again seemed to exhibit some distinctly flaky behaviour.

After a complex installation process, thanks to the test lab's lack of an outside connection and the need to update various components manually, the on-demand scanning seemed not to work, both from the 'custom scan' area of the main interface and from the context menu option. This oddity was quickly resolved by starting a full system scan, which worked without a hitch, then stopping it; the other scanning options suddenly became properly responsive.

Configuration was pleasingly thorough, although the custom scan did insist on checking the memory, registry and system areas each time, which became rather tiresome when running a series of small quick scans as part of the speed test, and rendered gathering times for these scans somewhat inexact.

Despite this, scanning speeds turned out to be fairly good and detection rates were reasonable, but a small number of file infectors were missed in the WildList set and a couple of items in the clean set were labelled as 'TROJ_Generic'. As a result *Trend* does not qualify for the VB100 award on this occasion.

VirusBuster Professional 6.0.191

ItW	99.99%	**Worms & bots**	100.00%
ItW (o/a)	99.99%	**Legacy**	99.98%
File infector	99.21%	**Polymorphic**	79.29%
False positives	0		

A much more pleasant experience was had with *VirusBuster*. The installation process sped through in a few steps from the admin password, via a licence code to full operation in a few moments. The interface is a tried and trusted one – not a favourite thanks to a little complexity in the on-demand task design, but perfectly usable and logically designed. Scanning was remarkably speedy and configuration plentiful, although the addition of 'all files' to the on-access mode apparently did not cover archive types.

The manual scans were a little difficult to monitor, presenting no information on their progress; the only way to tell when one was finished was to watch the greyed-out buttons for a return to normal.

Detection was at its usual fairly high level, but as expected from testing a few other products using the same detection technology this month, a small handful of samples from one of the expanded sets of W32/Virut samples – a different strain this time from those causing trouble for most other products – went undetected, and *VirusBuster* misses out on a VB100 award.

Webroot Spy Sweeper with AntiVirus 5.5.7.124

ItW	99.997%	**Worms & bots**	100.00%
ItW (o/a)	99.997%	**Legacy**	99.98%
File infector	100.00%	**Polymorphic**	100.00%
False positives	0		

Webroot is by tradition an anti-spyware product and thus operates in a slightly different style from the majority of other products on test; like some of the other products its on-access detection is not always sparked by simple file access, and had to be measured by copying the collections to the system. Some scanning of file accesses did seem to be happening though, judging by the slight delays running over the clean sets. These scanning speeds are recorded for interest, but do not represent full scanning.

On demand things were pretty speedy, and scans were completed without much difficulty despite there being a shortage of configuration options. Once the logs had been tracked down, the results were processed and tallied pretty closely with those of the *Sophos* engine powering the product. Unfortunately the similarity extended to the pair of missed Virut samples which also upset *Webroot*'s efforts to earn another VB100.

UNTESTED PRODUCTS

With the exceptionally large number of products taking part this month, a few problems along the way were only to be expected. Most products were eventually coaxed into producing some usable results, but a handful were left by the wayside after taking up more than their fair share of testing time.

A regular participant in recent tests, *iolo AntiVirus* was provided initially as a full version with licence code; unfortunately this version needed access to the Internet to further validate the installation. A plea to the developers brought forth a second version with the option of running in temporary trial mode, and this at least reached the installation stage. Once up and running, however, it insisted that the trial allowance had expired in mid-2007 (despite the build apparently dating from late February 2008); repeated retries failed to persuade the product to enable its protection features, and with many more products jostling for space on the test bench I decided regretfully to spend no further time on *iolo* this month.

As mentioned earlier, a second *ClamAV*-based product was also entered for the test, a fully open-source project called *Moon Secure Anti-Virus* with the delightful tagline 'Anti-Virus from Space'. The product proved well designed, reasonably stable and easy to use, but had been set up such that its on-access scanning would activate only on full execution. The hard-working developers quickly provided patches to enable full on-read scanning, but time was closing in and when these could not be made to work after a couple of attempts it was decided that *Moon Secure* would have to wait a couple of months before its full debut in the VB100 comparative – which should allow the developers sufficient time to perfect their product.

PC Tools submitted two products to this month's test. Alongside the straight anti-virus product was submitted the better-known *Spyware Doctor* with additional anti-virus functionality. This seemed to operate in a similar fashion to its stablemate and *Moon Secure*, with on-access scanning activated only when fully executing samples, and again the options to adjust this did not seem to function properly. As running each sample in all our infected and clean sets would be an enormously complex and time-consuming task, and as *PC Tools* already had a product successfully put through the testing process, it was decided that *Spyware Doctor* should also be dropped from the test, having taken up enough testing time unprofitably.

As these products fell into the category of 'untestable' no judgement can be given on their performance, and they will not be counted as entries in the VB100 history listings.

CONCLUSIONS

Another bumper crop of products and another draining month of intensive testing to a tight deadline.

Again a large number of issues have emerged from the test, most of them caused by a few variants of polymorphic file infectors, some of which have been resident on the WildList for some months and are now represented in greater numbers in the test set to provide a more accurate indication of detection rates. These sets, some of which previously contained only a handful of samples, now contain at least 50 and in some cases 100 or more; I would like to have each polymorphic item in the test sets represented by at least 500 samples, and over time will continue to expand the sets until they reach this sort of level. With many of these items continuing to trip up a variety of products, it seems sensible to have them as thoroughly represented in the test sets as possible.

Issues of stability and unexpected behaviour also caused problems this month, many of which seem likely to be a result of the updated platform. Hopefully many of these issues will be resolved as the service pack becomes more widely implemented by users and more fully tested by developers.

For me, the biggest headache of all was the sheer scale of the test, with a massive 40 products taking part. While a few of these didn't quite make it to the final line-up, they still took a hefty share of testing time, each having been given several retries before being deemed untestable. With a final total of 37, the field shows no signs of shrinking, and the test on *Windows XP* coming up in the summer looks likely to be even more heavily subscribed than this one – unless the developers are scared off by the rash of failed products this time around.

Technical details:

Tests were run on identical machines with *AMD Athlon64* 3800+ dual core processors, 1 GB RAM, 40 GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, all running *Microsoft Windows Vista Business Edition SP1* (32-bit).

Any developers interested in submitting products for VB's comparative reviews (and VB100 certification) should contact John Hawes on john.hawes@virusbtn.com. The current schedule for forthcoming VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.