COMPARATIVE REVIEW

WINDOWS VISTA X64 BUSINESS EDITION

John Hawes

After the enormous number of entrants for the last VB100 comparative review (see *VB*, June 2007, p.10), I was hoping for a quieter time this month. *Vista* is still pretty new, and the 64-bit version would, I hoped, pose enough difficulties to frighten off all but the most serious (or foolhardy) of vendors. The operating system promised no shocks for me, having gained some experience with its 32-bit sister in the early days of its release, but I was pretty sure that at least some of the products submitted would exhibit those quirks which seem just about compulsory on new platforms.

The range of products submitted offered few surprises. With 20 entries, the comparative proved a little more popular than I had expected, but there were no brand new faces this time, with most of the field made up by the group of familiar names that rarely miss a VB100.

PLATFORM AND TEST SETS

64-bit *Vista* is, on the surface, no different from the 32-bit version used in the February tests (see *VB*, February 2007, p.14), and as identical hardware was used the experience of building the test systems for this comparative had more than the usual number of déjà vu moments. Under the bonnet the differences should be fairly minimal, with compatibility generally not supposed to be an issue, although much debate raged in the months prior to the platform's release over access to the 'PatchGuard' kernel protection system and other additional security measures added to *Vista* on 64-bit architectures. Added to the User Access Controls, which caused a few wobbles in the earlier test, these new items could be expected to upset at least some functionality, and I could only hope nothing would seriously impede the process of ploughing through all the tests.

Installing was a pleasantly speedy process, accompanied by the flashy visual gimmicks that typify the platform, and previous experience once again helped steer a course around the small changes that hide most of the system configuration tools. After the eye-straining experience of the earlier *Vista* test, I reverted to Luddite principles and set all the display options to '*Windows* Classic' styles, eschewing the luminous and the curvy in favour of familiar, boxy grey windows and menus. Otherwise no changes were made from the default setup other than configuring networking.

The April 2007 WildList was used for this test, which added fairly few new items to the current mix – a scattering of the regular names, W32/Bagle, W32/Netsky and so on, plus some new variants on the same theme and a reappearance of a real old timer, W32/Sober. A pretty large swathe also fell off the list this month, including several varieties of the W32/Looked infectors which only joined the list in the last few months; considerable numbers of the W32/Mytob, W32/Rbot, W32/Stration and W32/Sdbot variants which make up the bulk of the WildList also fell to one side.

Other test sets were added to in a small way, mostly by the expansion of polymorphic sets, but the biggest changes were made in the clean and speed sets, with a large swathe of items added. The additions mainly comprised popular home-user software gathered from the web, but also a sizeable set of business and development tools and products, from *Microsoft* among others. These added a large number of installers and packages to the archive set, and the expanded contents to the various other sets as appropriate.

One item from amongst the stash turned out to be a 'legitimate' keylogger tool which was, of course, deemed inappropriate for the speed tests. Having backed up the sets ready for testing, the first run revealed that the installer had failed to be removed from the false positive set, so it remained throughout the tests and became an interesting indicator of which products were covering this kind of unpleasantware.

Alwil avast! Professional 4.7.1015

ItW	100.00%	**Worms & bots**	99.77%
ItW (o/a)	100.00%	**DOS**	99.34%
File infector	98.39%	**Macro**	99.56%
Polymorphic	85.94%	**False positives**	0

Alwil's product started things off in the manner I expected things would carry on – with one of *Vista*'s endless queries about whether I really wanted to install this software from an unknown publisher. These queries are, of course, a security measure, but it is hard to avoid the conclusion that most users, bombarded with these popups, blocks and queries, will soon tire of them, cease to read the scant details provided and click 'OK' without further thought. Critics of the 'warning – are you sure?' method have argued that these systems do little more than indemnify *Microsoft* from accusations of failing to secure its operating system, passing all blame onto the foolish end-user, while I have often felt the sneaking suspicion that they have been put there merely to irritate people testing large numbers of software products.

vb 100 VIRUS virusbtn.com Aug 2007

Once the smooth and speedy install was done and the system rebooted, yet another popup demanded to know if I really meant to open the *avast!* interface, then I finally got to play around with it. Skipping straight past the stylized

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.
Alwil avast!	0	100.00%	1	99.77%	236	99.34%	14	97.97%	18	99.56%	268	85.94%		2
Bullguard	0	100.00%	0	100.00%	11	99.44%	3	98.32%	22	99.46%	10	97.91%		
CA eTrust	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
CAT Quick Heal	0	100.00%	0	100.00%	1103	91.39%	23	96.16%	82	98.04%	388	76.99%		
ESET Nod32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Fortinet FortiClient	1	99.97%	1	99.97%	0	100.00%	2	99.52%	821	81.05%	56	94.99%	1	
G DATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		2
Grisoft AVG	0	100.00%	3	99.59%	197	99.10%	16	97.10%	3	99.93%	194	76.46%		
Ikarus Virus Utilities	0	100.00%	1	99.92%	2119	92.93%	42	93.92%	174	95.94%	399	71.81%	46	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	2	99.52%	0	100.00%	0	100.00%		
Kingsoft Internet Security	0	100.00%	429	14.33%	12937	55.59%	192	70.13%	463	89.92%	2202	31.90%		
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%	0	100.00%	0	100.00%	5	98.62%	0	100.00%	29	96.30%		
Microworld eScan	0	100.00%	0	100.00%	0	100.00%	1	99.28%	15	99.69%	0	100.00%		
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	0	100.00%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Trend Micro Client Server Security	0	100.00%	0	100.00%	744	98.39%	15	97.80%	13	99.68%	152	93.29%	1	
Trend Micro OfficeScan	0	100.00%	0	100.00%	744	98.39%	15	97.80%	13	99.68%	152	93.29%	1	
Trend Micro PC-cillin	0	100.00%	0	100.00%	744	98.39%	17	97.32%	13	99.68%	152	93.29%	1	
VirusBuster VirusBuster	0	100.00%	1	99.97%	20	99.77%	11	98.08%	0	100.00%	98	88.22%	1	4

basic version of the GUI, which I imagine may be quite simple to use for those practised in its intricacies but remains almost entirely baffling to me, I delved into the advanced version for most of my testing needs. From here settings can be changed by adjusting the properties of various ‘tasks’, and some tweaks to the settings of the ‘resident protection’ (on-access) and ‘interactive scan’ jobs proved adequate for most of the tests.

During on-demand scanning, the window area showing the status and results of the scan was a little wobbly, starting out completely blank and remaining so until some judicious jiggling of the scroll bars brought the information out of hiding. This allowed me to track the progress of scans and gather results, which showed pretty solid detection across all sets and decent speeds in the default settings, which do not include delving into compressed archives. With archive scanning enabled, things slowed to a bit of a crawl, particularly with a couple of .jar files which eventually had to be removed from the set to allow the scans to complete in reasonable time.

This aside, detection in the WildList proved faultless, and with just a joke program and a risky tool spotted in the clean sets, *avast!* easily picks up another VB100 award.

Bullguard v.7.0 x64

ItW	100.00%	**Worms & bots**	99.77%
ItW (o/a)	100.00%	**DOS**	99.77%
File infector	98.32%	**Macro**	99.69%
Polymorphic	97.94%	**False positives**	0

Plucky *Bullguard* stormed to victory in the June *XP* comparative (see *VB*, June 2007, p.10), seizing a well deserved VB100 award at first attempt. Returning for a second time, the product seemed much the same – slick and smoothly laid out and adorned with numerous wrinkly-faced pooches. The installation procedure requests a web-based login process to ‘activate’ the product, but this can be skipped to give a seven-day ‘grace period’. The main product interface is a pretty affair, glossy and colourful and featuring some pleasantly quirky, friendly comments scattered amongst the more serious business of malware protection.

Operation was fairly straightforward, with configuration options not enormously granular but with most things required by the average home user amply covered.

Right-click scanning was available, but only functions in fully activated products, so I was reduced to using the interface itself for the on-demand tests – no great disaster really as the scanning section is as clearly designed as the rest of the GUI. Speeds were fairly good, considering the depth of scanning going on, and that rogue keylogger that crept into the clean set was spotted, and identified as containing both spying and hiding techniques.

An initial submission of the product proved to be a faulty build, missing a vital component which rendered the on-access scanner inactive after scanning 255 files. However, a fully working replacement suffered no such problems, and a suspected false positive in one of the clean sets, a file labelled as a spyware-doctored hosts file, proved to be a database of such subverted hosts files used by a security product, and was thus stricken from the test set. With no other problems, *Bullguard* earns itself a second VB100 award.

CA eTrust r.8.1.634.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	N/A	**DOS**	99.67%
File infector	99.38%	**Macro**	99.82%
Polymorphic	99.85%	**False positives**	0

CA's *eTrust* has a long and solid history in VB100 comparative testing. *CA*'s traditional submission method has been to provide a CD, or CD image, each time a major update to the main product is released, and in between simply to send in definition updates for each review. For this test, however, the submission method proved not to be good enough, with the 8.1 build which had been sitting cosily in the *VB* lab since the new year, proving inadequate for the demands of 64-bit *Vista*. The installer began its business happily, let me go through the lengthy process of scrolling through several sizeable EULAs and filling in lots of required user information, then quietly freaked out and froze. After some frantic pestering a more suitable version was eventually provided by the vendor, just in time to make the cut for this comparative.

The 64-bit version proved more effective, and after yet another run through the arduous install process I was able to get my hands on the product itself. The browser-borne GUI, usually a slow and unwieldy thing, was considerably more responsive than usual under 32-bit *Vista* earlier in the year, but any hopes of a repeat performance were soon dashed, and several long sessions of staring at the progress bar seemed to augur badly for the rest of the test. Fortunately, I discovered the right-click scanning option opened a mini-interface of its own, which was nice and simple and responsive, and carried enough configurability to run through the on-demand tests with ease. Detection was in the upper range as expected, and speeds were impressively zippy.

Moving on to the on-access side of things, speeds were even more remarkable. Suspiciously so, in fact. Trying the on-access detection test revealed something was seriously wrong – nothing seemed to be detected at all. I tried numerous methods beyond the simple opener tool which usually suffices to exercise *CA*'s products, but copying files around the system, and even dropping them in from the network, sparked neither blocking nor alerting. Several reinstallations on fresh systems failed to make things any better, and I was on the verge of despair when I discovered the root cause.

During on-demand speed testing, I had observed that checking the 'scan archives' box on its own had no effect, as the list of archive types remained unchecked – once all of these were selected, archives were indeed scanned internally. Changing some settings in the on-access controls, which sadly meant resorting to the full ITM interface, I found scanning suddenly worked fine; with 'scan all files' active, normal scores were recorded in all infected sets. It emerged that the default setting, targeting only a pre-defined list of extensions, was failing to work because the pre-defined list was entirely empty.

This being the default setting, testing could not successfully be carried out under the rules of the test, but hopefully most administrators would spot this flaw before deploying the software to their 64-bit *Vista* users. Nevertheless, it is enough of a problem to deny *CA* a VB100 award this time, and to keep its spectacular speed settings from cluttering our speed graphs.

CAT Quick Heal 2007 v.9.00

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	95.06%
File infector	97.00%	**Macro**	98.18%
Polymorphic	76.99%	**False positives**	0

CAT's *QuickHeal* installs as swiftly as its title implies, with nothing to tax the mind along the way, and the clear and well laid out interface is equally speedy to navigate, responsive and stable throughout the tests. The welcoming purple blob planted in the system carries a pleasant message congratulating the user on their choice of security software, and the whole product is set out in a similarly user-friendly manner.

vb 100 VIRUS virusbtn.com Aug 2007

A few oddities were encountered during testing: logs seemed to take a long time to export to file and the switch

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.
Alwil avast!	0	100.00%	1	99.77%	236	99.34%	12	98.39%	18	99.56%	268	85.94%		2
Bullguard	0	100.00%	1	99.77%	15	99.77%	3	98.32%	13	99.69%	5	97.94%		
CA eTrust	0	100.00%	0	100.00%	235	99.67%	3	99.38%	12	99.82%	2	99.85%		
CAT Quick Heal	0	100.00%	0	100.00%	1054	95.06%	20	97.00%	73	98.18%	388	76.99%		
ESET Nod32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	
G DATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		4
Grisoft AVG	0	100.00%	2	99.69%	197	99.10%	14	97.58%	0	100.00%	194	76.46%		
Ikarus Virus Utilities	0	100.00%	1	99.92%	2119	92.93%	42	93.92%	158	96.27%	399	71.81%	46	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Kingsoft Internet Security	0	100.00%	429	14.33%	12937	55.59%	192	70.13%	463	89.92%	2202	31.90%		
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%	0	100.00%	0	100.00%	3	99.10%	0	100.00%	29	96.30%		
Microworld eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	0	100.00%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Trend Micro Client Server Security	0	100.00%	0	100.00%	233	99.47%	9	99.24%	13	99.68%	152	93.29%	1	
Trend Micro OfficeScan	0	100.00%	0	100.00%	744	98.39%	15	97.80%	13	99.68%	152	93.29%	1	
Trend Micro PC-cillin	0	100.00%	0	100.00%	233	99.47%	9	99.24%	13	99.68%	152	93.29%	1	
VirusBuster VirusBuster	0	100.00%	0	100.00%	20	99.77%	8	99.28%	0	100.00%	98	88.22%	1	4

from the main interface to the configuration area brought about one of those flashes of blackness which seem a regular occurrence under *Vista*, but other than these there was nothing to detract from the overall pleasant experience of using the product.

Scanning speeds were as decent as expected, although the option to scan inside archives and otherwise expand the scope of the on-access mode was notably absent, and while detection over the older sets remains less than flawless nothing was missed in the newer areas, including the WildList. With no false positives generated in the clean set, *QuickHeal* earns itself another VB100 award.

ESET Nod32 Antivirus System v.2375

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

ESET's upcoming overhaul of its product has yet to reach the *VB* test bench, so once again the tests were run with the familiar interface which has graced every *Windows* test of my reign here. The product's current design loses a lot of its glamour in the more glossy environment of *Vista*, but practice has nullified its oddities, which are mostly confined to identifying its component modules by inscrutable acronyms, and the interface has become a pleasure to use.

Tweaking the settings of 'AMON' and the right-click scan 'profile' to my needs, all the tests were carried out quickly and easily, testament to the solidity and lightning scanning speed of the engine powering the product as much as to the usability of the interface.

Speeds were a little less eye-opening than usual over the much expanded archive set. On-access settings cannot be expanded to cover the full range of files scanned on demand, and the product threw up some errors scanning the master boot records of my hard drives, but beyond these minor quibbles detection was as unimpeachable as ever. With nothing missed in any set and not a shadow of a false positive, *ESET* earns yet another VB100 award to add to its sizeable stash.

Fortinet FortiClient 3.0.458

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	99.97%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	1

FortiClient is another product that has changed little since I first encountered it, on the surface at least. Its busy interface covers a wide range of functionality, arranged into a long row of tabs squeezed down the left-hand side of the window and each further divided into more tabs for configuring and checking the status of each area. This wide range of functions caused even more questioning from *Vista*, with numerous confirmations required to install the various drivers etc. required by the product.

On-demand results were as comprehensive as ever, and scanning speeds were fairly decent, with particular thoroughness shown to the executable set, where a single item, part of a PDF creation utility, was flagged as vaguely 'suspicious'. Under the tightened rules of the VB100 such a slander on a file's reputation is adjudged enough to disqualify a product from the award.

This would have seemed rather a cruel treatment of a solid product had not a change to the default on-access settings, from 'all files' to only 'programs and documents', meant that besides large numbers of macro and polymorphic samples being missed thanks to the omission of .xls and .xlt files from the document set, a single WildList sample, W32/Funlove in .ocx format, was also passed over. Although detection for all these items was clearly in place, the VB100 rules insist on using default settings at all times, and it appears that in an attempt to improve its on-access performance, *Fortinet* may have reduced its coverage a little too far.

G DATA AntiVirusKit 17.0.7171

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

G DATA's *AVK* has a very slick appearance, and equally smooth and impressive detection powers. The interface is clearly laid out, allowing all the required configuration for my needs without appearing too complex or technical for the average user. It has performed excellently in the last few tests with barely a slip or stumble to report.

This time, after installation and a reboot, things were as solid and stable as ever, with no surprises or annoyances beyond the rather odd habit of opening new instances of the interface each time the handy context-menu scan is used, leaving several strewn about the screen if a forgetful tester omits to shut them down. Logging was slightly pesky, with file names separated from their paths, but for those real-world people not needing to extract large amounts of data this is probably an extra touch of clarity and thoughtful design.

For a multiple-engine product, speeds were pretty decent in most sets, though the archive collection did take some serious time to slog through – the product helpfully warns about potential slowness if no maximum depth of archive scanning is set. The keylogger that slipped into the clean set was spotted – described as a 'monitor', 'Not-a-virus' – as well as a joke program, an *IRC* client and some 'Risktools', but nothing marred the superb detection and *G DATA* earns another VB100 award.

Grisoft AVG Professional Edition 7.5.476

ItW	100.00%	**Worms & bots**	99.69%
ItW (o/a)	100.00%	**DOS**	99.10%
File infector	97.58%	**Macro**	100.00%
Polymorphic	76.46%	**False positives**	0

Grisoft's *AVG*, wildly popular with the home-user market thanks to the broad availability of its free version, remains a solid performer, and its installation was another simple and painless experience. The user interface itself is divided into simple and advanced versions, and while doubtless more than adequate for the needs of most, has always proved a little confusing when more in-depth configuration is required to smooth the passage of a test, but familiarity with its rather esoteric layout has improved matters considerably.

Speeds were on the slow side, but on-access overheads were considerably better than the more thorough on-demand settings; detection rates were similarly solid, if not flawless, and without a miss in the WildList set or a false positive to mark it down, *Grisoft* also makes the grade for the VB100.

Ikarus Virus Utilities 1.0.57

ItW	100.00%	**Worms & bots**	99.92%
ItW (o/a)	100.00%	**DOS**	92.93%
File infector	93.92%	**Macro**	96.27%
Polymorphic	71.81%	**False positives**	46

Ikarus returned to the *VB* test bench in the June *XP* comparative after a nearly six-year absence, with a new

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)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
Alwil avast!	136	15.05	610	3.36	211	12.02	245	10.35	109	13.81	132	11.40	57	11.85	67	10.08
Bullguard	2386	0.86	2386	0.86	321	7.90	321	7.90	80	18.81	80	18.81	103	6.56	103	6.56
CA eTrust	14	146.22	706	2.90	55	46.10	61	41.57	23	65.43	24	62.70	20	33.77	22	30.70
CAT Quick Heal	497	4.12	823	2.49	66	38.42	67	37.85	49	30.71	49	30.71	38	17.77	39	17.32
ESET Nod32	726	2.82	726	2.82	270	9.39	270	9.39	32	47.03	32	47.03	25	27.02	25	27.02
Fortinet FortiClient	342	5.99	342	5.99	565	4.49	565	4.49	38	39.60	38	39.60	34	19.87	34	19.87
G DATA AntiVirusKit	1987	1.03	3402	0.60	337	7.52	338	7.50	94	16.01	119	12.65	78	8.66	133	5.08
Grisoft AVG	2246	0.91	2246	0.91	315	8.04	315	8.04	133	11.33	133	11.33	16	41.45	16	41.45
Ikarus Virus Utilities	124	16.51	339	6.04	200	12.68	208	12.19	39	38.59	41	36.71	70	9.65	70	9.65
Kaspersky Anti-Virus	74	27.66	1299	1.58	54	46.96	182	13.93	65	23.15	71	21.20	48	14.07	59	11.45
Kingsoft Internet Security	679	3.01	679	3.01	257	9.87	257	9.87	69	21.81	69	21.81	78	8.66	78	8.66
McAfee VirusScan	628	3.26	628	3.26	322	7.88	322	7.88	46	32.72	46	32.72	53	12.74	53	12.74
Microsoft Forefront	550	3.72	550	3.72	195	13.00	195	13.00	54	27.87	54	27.87	32	21.11	32	21.11
Microworld eScan	1401	1.46	1401	1.46	460	5.51	460	5.51	276	5.45	276	5.45	280	2.41	280	2.41
Sophos Anti-Virus	23	89.00	713	2.87	217	11.69	234	10.84	37	40.67	54	27.87	29	23.29	65	10.39
Symantec AntiVirus	450	4.55	450	4.55	169	15.00	169	15.00	53	28.39	53	28.39	44	15.35	44	15.35
Trend Micro Client Server Security	74	27.66	79	25.91	167	15.18	169	15.00	21	71.66	22	68.41	30	22.51	32	21.11
Trend Micro OfficeScan	96	21.32	209	9.79	201	12.62	218	11.63	38	39.60	38	39.60	35	19.30	43	15.71
Trend Micro PC-cillin	203	10.08	212	9.66	180	14.09	183	13.86	26	57.88	26	57.88	30	22.51	34	19.87
VirusBuster VirusBuster	262	7.81	607	3.37	322	7.88	323	7.85	26	57.88	54	27.87	16	42.22	39	17.32

product in the later stages of development. On that occasion the product showed signs of needing a little more work. The submission method was a little different this time, with a CD image provided rather than the bare bones of the product itself. This smoothed over a few of the wrinkles previously experienced in the installation process – the requirement for the *.NET* framework, in this case installed automatically as part of the setup process, being the most obvious.

Running of the product itself, after an apparently unstoppable attempt to contact the web to update, had also improved considerably. Double-clicking the desktop icon at first had no effect, leading to fears of a repeat of earlier problems with starting the GUI, but it proved just to be rather slow to open. Some of the language used is rather odd, and occasionally seems misleading – the on-access monitor reports it is 'inactive' if automatic updating is not running, which may actually be a useful warning to users that running out-of-date software is a dangerous state to be in.

There were a few further problems with the responsiveness of the interface during the more stressful of the detection tests; things faded out while scanning the infected collections and again after I foolishly clicked the 'quarantine' button with several thousand files waiting to be dealt with. The results showed that, while detection across the zoo collections was a little lacking, the WildList set was fully covered in both modes.

Hopes that *Ikarus* may have qualified for its first VB100 were dashed in the clean sets however; speeds were perfectly reasonable throughout, and outstanding in some sets, but the scans were marred by a scattering of false positives across several of the sets. The much improved product will surely make the grade sometime soon.

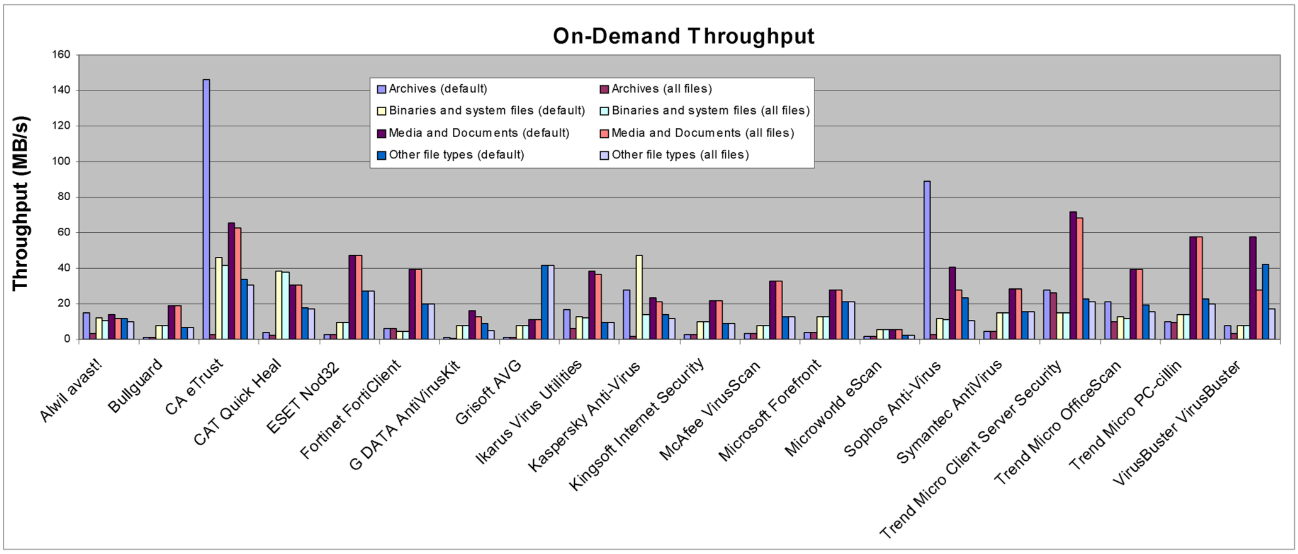
Kaspersky Anti-Virus 7.0.0.123

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

Version 6 of *Kaspersky*'s product has put in some sterling performances in VB100 testing over the last year or so (a momentary lapse which denied it the award in the last test notwithstanding), and the product impressed me considerably in a more thorough standalone review some months ago. Now it has been superseded by a new edition, with some serious redesign work having been put into the appearance of the product.

vb Aug 2007 100 VIRUS virusbtn.com

The install process looked somewhat shinier, but also felt a little slow moving, and required a reboot to complete. The new interface was considerably more glossy than the



previous incarnation, and has lost the cuddly, cartoon-like appearance in favour of a more high-tech, space-age theme.

The redesign has not reduced the fine-grained configurability of the product, or the solid thoroughness of the detection – a thoroughness which is reflected by the speed measurements, particularly with archive scanning enabled. No false positives and immaculate detection levels, barring a couple of files in formats not scanned by default on access, brings *Kaspersky* back to the podium as a VB100 winner.

Kingsoft Internet Security 2007.6.21.206

ItW	100.00%	**Worms & bots**	14.33%
ItW (o/a)	100.00%	**DOS**	55.59%
File infector	70.13%	**Macro**	89.92%
Polymorphic	31.90%	**False positives**	0

Kingsoft makes its second attempt at the VB100 this month, having first entered several months ago (see *VB*, October 2006, p.10). The product's earlier appearance was marred by a small number of misses in the WildList test set and a fair number of false positives, but the company has reportedly been working hard to resolve these issues in preparation for its latest submission.

Running through the installer and the process of navigating around the product proved a happy experience, with everything running smoothly and slickly with a minimum of pestering from *Vista*. A problem encountered previously, with the log display interface lacking translation and crashing out when a log was selected, proved avoidable by the simple expedient of switching the system locale from the UK version usually used in *VB* tests to the more standard US setting.

Speeds in the clean sets were good, and no false positives were flagged in any of the newly enlarged sets. In the infected sets, detection rates were low and in some cases very low – most worryingly in the worms and bots set which contains the newest material, much of it recently downgraded from the WildList. *Kingsoft*'s developers have clearly been focusing closely on the WildList itself, however, and much to their credit the product managed to cover the whole set, earning it a VB100 award at its second attempt.

McAfee VirusScan Enterprise v.8.5I

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 corporate product remains its familiar self, somewhat severe and serious in appearance and reliable in performance. The installer was slick and problem-free, with no reboot required, but to open the interface required yet another confirmation dialog every time, which proved a little annoying.

A previous annoyance, that the control to disable and activate the on-access scanner could not be run from the interface but required using the system tray menu, has been resolved in this version, speeding the tests along nicely, and with decent speeds and flawless detection, *McAfee* wins itself another 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 - default	
	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)
Alwil avast!	49	0.02	1410	0.69	223	0.08	252	0.09	120	0.07	133	0.08	59	0.07	58	0.06
Bullguard	111	0.05	1152	0.56	297	0.11	341	0.13	82	0.04	96	0.05	109	0.14	119	0.16
CA eTrust	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
CAT Quick Heal	20	0.01	N/A	N/A	67	0.02	N/A	N/A	26	0.01	N/A	N/A	18	0.01	N/A	N/A
ESET Nod32	8	0.00	N/A	N/A	60	0.02	N/A	N/A	47	0.02	N/A	N/A	36	0.03	N/A	N/A
Fortinet FortiClient	89	0.04	119	0.06	334	0.12	591	0.23	29	0.01	35	0.01	33	0.03	48	0.05
G DATA AntiVirusKit	156	0.07	779	0.38	347	0.13	366	0.14	158	0.10	163	0.10	96	0.12	99	0.13
Grisoft AVG	17	0.01	N/A	N/A	133	0.05	N/A	N/A	29	0.01	N/A	N/A	16	0.00	N/A	N/A
Ikarus Virus Utilities	131	0.06	341	0.17	232	0.08	237	0.09	54	0.03	56	0.03	86	0.11	89	0.11
Kaspersky Anti-Virus	20	0.01	158	0.08	190	0.07	209	0.08	77	0.04	92	0.05	52	0.06	77	0.09
Kingsoft Internet Security	39	0.02	N/A	N/A	141	0.05	N/A	N/A	80	0.04	N/A	N/A	88	0.11	N/A	N/A
McAfee VirusScan	30	0.01	304	0.15	330	0.12	330	0.12	57	0.03	56	0.03	61	0.07	62	0.07
Microsoft Forefront	27	0.01	N/A	N/A	218	0.08	N/A	N/A	63	0.03	N/A	N/A	46	0.05	N/A	N/A
Microworld eScan	764	0.37	764	0.37	371	0.14	371	0.14	179	0.11	179	0.11	158	0.21	158	0.21
Sophos Anti-Virus	24	0.01	559	0.27	212	0.08	228	0.08	39	0.02	53	0.03	33	0.03	60	0.07
Symantec AntiVirus	16	0.01	N/A	N/A	135	0.05	N/A	N/A	36	0.01	N/A	N/A	34	0.03	N/A	N/A
Trend Micro Client Server Security	68	0.03	77	0.04	200	0.07	203	0.07	67	0.03	69	0.04	40	0.04	51	0.05
Trend Micro OfficeScan	67	0.03	69	0.03	182	0.07	183	0.07	51	0.02	52	0.02	48	0.05	52	0.06
Trend Micro PC-cillin	26	0.01	219	0.11	153	0.05	172	0.06	36	0.01	49	0.02	34	0.03	45	0.05
VirusBuster VirusBuster	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

Microsoft Forefront Client Security 1.5.1937.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	99.10%	**Macro**	100.00%
Polymorphic	96.30%	**False positives**	0

Microsoft's corporate security product is designed to be installed and managed from a central server, the requirements for which run beyond the space provided for this review, but standalone running is available, albeit with a rather unusual, almost silent installation process.

Once up and running, *Forefront* has a fairly simple, pared-down interface, with most of the configuration presumably left for the centralized control utility. Unsurprisingly, it looks much like a part of the operating system, and does its job quietly and efficiently. Speeds were decent, and detection pretty good, with recent efforts to improve coverage of the *VB* test sets paying off and leaving little unidentified.

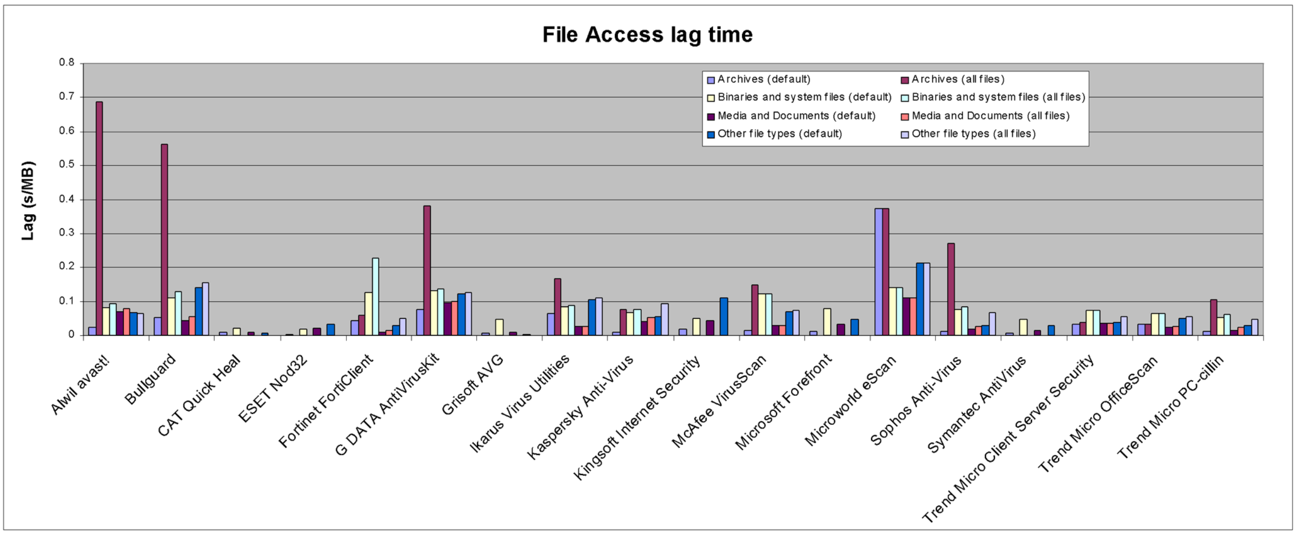
A strange issue with a single item in the WildList, for which the default setting appears to be to allow it to run when detected, was spotted in the previous test (see *VB*, June 2007, p.10) and still seems to be in evidence. However, on a second run through, with on-demand scanning performed before on-access scanning, the application of the on-demand actions seemed to change things and access to the file was subsequently blocked. The file was invariably detected however, and with nothing in the WildList missed, and no false positives, *Forefront* is deemed worthy of its second VB100 award.

Microworld eScan Internet Security for Windows 9.0.722.1

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

Microworld's *eScan* boasts of being 'powered by *Kaspersky*', and adds a few treats of its own to the hired-in malware scanning. The installer offers a 'Lite' version of a management interface, designed to manage several systems on a small network, while population of an anti-spam whitelist is offered along with the other setup tasks, which include an automatic attempt to update.

As an interface to the *Kaspersky* engine, *eScan* has a few issues on this platform; the popup 'are you sure?' queries are in evidence each time the product is run, and even more



intrusively each time a right-click scan is attempted, with the black screen that precedes many of these popups causing regular moments of concern. The right-click scans themselves seemed not to work at all, unless they run silently and with no logging, which would be of little use to most users.

Scanning from the main interface did work however, and the tests were conducted in this manner, with some slowish speed times reflecting the depth of scanning going on. The expected thoroughness of detection was mostly in evidence, although a handful of macro samples were rather inexplicably missed on access. Nothing was missed in the WildList test set however, and without false positives and with the rogue keylogger left in the clean set spotted, *eScan* battles through to achieve another VB100 award.

Sophos Anti-Virus 7.0.0

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

Like *Kaspersky*, *Sophos* has upgraded from version 6 to version 7 for this test, a change coinciding with the company's acquisition of a NAC provider. The change in version has had a far less dramatic effect on the product's interface however, which remains pretty much as it was. Once installed, the running of the software is once again impeded by *Vista* warning popups, which (again) frustratingly extend to each time a scan is run from the context menu option. This little annoyance aside, configuration remains flexible in-depth, detection and speeds very good throughout, with a few items in the clean set adjudged risky to corporate networks and the keylogger tool flagged as a possible trojan.

With no misses or false positives *Sophos* also proves worthy of a VB100 award this month.

Symantec AntiVirus 10.2.0.298

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

Symantec's corporate product was one of few to require its installer to be run with full administrator rights, but less complex tweaking of the user access controls was required this time than in the earlier *Vista* test, and soon another familiar interface presented itself for testing.

With the help of this familiarity, navigating the controls was a simple task, with the available options plentiful and accessible, and tests were run through without excessive difficulty. Scores were impeccable, including detection of the keylogger, and speeds were reasonable across the board; without a false positive or missed item of malware, *Symantec* earns itself yet another VB100 award.

Trend Micro Client Server Security for SMB 7.6.1095

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.47%
File infector	99.24%	**Macro**	99.68%
Polymorphic	93.29%	**False positives**	1

Trend saw fit to submit no fewer than three separate products for this month's test, the first of which is new to the *VB* test bench. The small business product is a notch below *OfficeScan* in the size of networks it is designed to manage, but operates in a similar way, with a central management console controlling desktop installations, and a simpler interface at the local system level.

Installing the product was simpler than previous experiences with *OfficeScan* had led me to fear – the whole thing installed on the local system, integrating the management tools with a local install in a single go. However, the installation process was not quite done with when, after several setup stages and a query from the *Vista* firewall about whether I wanted to allow the product's *Apache* server to start up, I got access to the interface itself, or rather themselves. For the first 20 minutes or so of using the product, searching for the option which would allow me to control the configuration of scanning and on-access protection from the simpler local console, the browser-based GUI was plagued with blocks from *IE7*'s security measures. *IE7* prompted initially that I should not visit the interface as its certificate was unrecognized, and several times required permission to install the many *ActiveX* controls used by various parts of the system.

When the controls were finally fully running, and control privileges passed to the local user, things became a lot easier, and I found the main interface itself fairly usable and responsive. On-demand scans, which can only be run over the full machine from the 'remote' interface, zipped through nicely, showing fairly solid detection levels, and I soon moved on to the on-access side of things. A repeat of earlier experiences with suspiciously fast run times over the clean sets ensued. After much checking and tweaking of options, I finally found that the on-access scanner was not being sparked by the basic opener tool used for the speed tests, and resorted to copying the collections from one drive to another to obtain detection results.

With the test sets moved to the C: drive, a rerun of the opener provided an odd result – detection was sparked by files being accessed in this manner, but only on the system drive. Unsure whether this was a performance-enhancing function or a bug, I queried it with the developers, who are investigating this oddity, but fortunately the discovery allowed the on-access detection and speed tests to be properly carried out, albeit in a slightly different location from that used elsewhere.

A question arose as to whether not spotting the malware on other drives constituted a failure to detect, but was quickly brushed aside with the justification that many products need a little coaxing to produce on-access results. Unluckily for *Trend*, however, a single item from the batch recently added to the clean set – a development tool provided by *Microsoft* – was falsely identified as spyware, spoiling *Trend*'s chances of a VB100 hat-trick before things had even got going.

Trend Micro OfficeScan 8.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	98.39%
File infector	97.80%	**Macro**	99.68%
Polymorphic	93.29%	**False positives**	1

OfficeScan is the big brother of the previous product, similar in design but clearly aimed at much larger organizations. In previous tests on 64-bit platforms, it has been necessary to set up a separate server machine on a 32-bit system and install to the test machine across the network. This proved unnecessary this time, with the management unit installing happily on the *Vista* system alongside the client.

The platform is not officially supported by *Trend*, but it worked well enough to perform the tasks previously deduced as necessary, delegating power to the local client to tweak settings as required. On-access scanning could not, without some complex fiddling, be entirely deactivated from the local console, but beyond that most of my needs were met by the smaller, nimbler interface.

Logging was the only issue which could not be thus circumvented, and a possible indicator of the management interface's unsupported status emerged when trying to save the logs from there, finding them to be somewhat truncated. Lacking the time and resources to set up a fully functioning management server, I made do with running several smaller scans and tagging the logs together. On-demand detection results were similar to those previously spotted, although some of the more venerable samples seemed to be missed, alongside a few other differences which can be accounted for by minor alterations to the defaults.

The problem with on-access scanning on other drives recurred, and further tests showed full detection when moving samples about between drives and writing them in across the network. WildList results were solid, but again a single false positive was raised by the spyware side of the product on access, denying *OfficeScan* its VB100 this time.

Trend Micro PC-cillin Internet Security 2007 15.30.1239

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.47%
File infector	99.24%	**Macro**	99.68%
Polymorphic	93.29%	**False positives**	1

On to the home-user product, and one whose interface does not require the installation of an endless stream of *ActiveX* controls. *PC-cillin* is a much more pleasant product to test, being aimed squarely at the home user rather than a corporate admin with a complex security policy to administer and plenty of time to get things set up.

The installation process and interface are simple and pleasant, with curvy lines and plenty of colour to keep the user on side, and while some options are lacking there is still plenty of tweaking available for those who need it. The most obvious shortcoming in all of the *Trend* submissions this month, as pointed out in a recent review of *PC-cillin*, is the lack of a right-click scanning option.

Once again everything went well on demand, and fell over somewhat on access. Scanning was once more most easily achieved on the C: drive, with copying around the system blocked but not, rather worryingly, when copying from a network share onto a local drive, even the system partition. Once again that single clean file was flagged on access, the on-demand virus scan not making use of the spyware engine, and despite decent detection rates *Trend* loses out on the chance of a VB100 award from its three submissions.

VirusBuster VirusBuster Professional 6.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.77%
File infector	99.28%	**Macro**	100.00%
Polymorphic	88.22%	**False positives**	1

VirusBuster's product is another that seems barely altered over its many appearances on the *VB* test bench, and the familiar installation ran through almost on auto-pilot. Setting up scans, run from the interface in the absence of a right-click option, remains a little taxing despite much practice. However, on-demand tests were soon out of the way – at least until I tried to save the log. Admittedly the log had grown to quite some size during the scanning of the infected sets but saving it nevertheless took an enormous amount of time – during which the interface was unusable.

On-access scanning again proved somewhat problematic, with the opener tool, usually perfectly adequate to test the product, not sparking any detection. Results were once again obtained by copying files around, which meant no comparable speed times could be obtained for this mode. Checking the results showed very good detection though, with nothing vital missed; however, several items in the clean set were flagged with the phrase 'exploit: attempt to crash system by archive'. While this alert was labelled an error rather than a malware warning, it seems severe enough also to count as a false alarm, which would lead users to delete valid files in the belief that they were some form of attack. The need to make a judgement on this difficult issue was postponed for another day, however, when an item in another part of the set was clearly labelled a virus, and *VirusBuster* thus misses out on an award.

CONCLUSIONS

With few additions to the WildList, and many items removed, the target for the VB100 seemed much easier to achieve this month. However, the rough terrain provided by the platform tripped up several products, with many suffering frustrations imposed by the locking-down of the operating system and others showing idiosyncrasies in their integration into it. On-access scanning, perhaps unsurprisingly, proved difficult to get right for many, while on-demand detection was barely affected by the change of setting.

Almost all of this month's failures were due to false positives, thanks in part to an enlargement of the clean test sets. The amount of data added was fairly trivial however, with perhaps 100 applications and their component parts added, a minute quantity in comparison with the vast amounts of software in use around the world. These were all fairly common items, mostly taken from the 'most popular' lists of several major free and free-trial download sites, and the resultant surge in false detections seems to indicate a fairly significant problem for anti-malware software.

The VB100 rules regarding false positives were changed for this test, with the 'suspicious' alert, which in earlier tests allowed products to warn of vague doubts about an item's intentions without penalty, now limited to covering only correct identifications of genuinely risky software. Hardly any of the products which failed this test did so entirely as a result of this change, but it has made an impact on the results for a few products.

Vista is fairly certain to be a major part of the future of computing, and x64 is also a growing trend with significantly more widespread uptake likely. While security vendors should hopefully be able to hone their wares to operate more smoothly and reliably on the platform before it becomes ubiquitous, it seems unlikely in these times of increasing reliance on heuristics that the false positive will ever be entirely eradicated. We must hope that, for the sake of user confidence in their security products, they can at least be kept to a minimum.

Technical details

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 Vista x64 Business Edition.*