COMPARATIVE REVIEW

MICROSOFT WINDOWS VISTA BUSINESS EDITION (32-BIT)

John Hawes

A new year, a new logo, a new platform, and the first of several planned changes to the VB100 test procedures have kept me busy this month. The initial excitement of finally getting my hands on *Vista* was tempered by a barrage of requests to postpone the test until certain vendors could get their products finalized, with many planning releases to coincide with the full commercial release of the new platform at the end of January. Many more vendors offered pre-release or beta products, while a handful had their *Vista* support well in order. Despite interest from several new vendors hoping for their products to join the tests, none were quite suited or ready in time, so this review saw no entirely new faces. Having said that, one considerably high-profile product returned this month for only its second visit to the *VB* test bench – its first since I took over – providing me with an extra tingle of anticipation.

A bumper set of additions to the WildList, including more of the file infectors which caused difficulties for some products last time around, added a further frisson of interest to get me through the mire of problems always associated with trying out a new platform and new procedures. Of course, once the troubles of setup were overcome, I faced a whole range of potential headaches while checking the various new and rejigged products submitted for the tests.

PLATFORM

The long-awaited *Microsoft Vista* is the first major new release of *Windows* since *XP* over five years ago (not counting *Windows Server 2003*, which was little more than a blending of *Windows 2000 Server* with some new *XP* ideas). Released to volume licensing customers late last year, the full commercial issue of the new platform coincides rather neatly with the publication of this issue of *VB*. The opportunity to allow our readers an early insight into how product developers have coped with the changes brought by the new platform seemed far too good to let pass.

The installation of *Vista* was a fairly pleasant experience, with the interface considerably improved; finally proper graphical screens present options and information in a visually appealing style, and the process itself was fairly speedy compared to my experiences of previous versions. Obviously the high specifications of the hardware I was using, and the speed of DVD reading compared to CD, more than counterbalanced the rather large 7GB of data put on my machine.

The system itself also aimed for visual appeal and impact, with everything colourful and shiny and vaguely reminiscent of another popular desktop system which has focused on style for some time now. Beneath the sheen of glamour, nothing had changed in too baffling a manner, with most of the required tools and settings in their usual, albeit somewhat prettified, places.

The only aspect I expected to cause any difficulty was the implementation of User Access Control (UAC), which even in the early stages reared its head a few times while getting things set up. Each machine was provided with a standard user in addition to the administrator and I planned, as far as possible, to install and test all products as this user, to give some indication of how products have integrated themselves into the UAC setup.

Once the operating system was installed and set up to my liking, it became clear fairly quickly that the aged imaging system I inherited in the *VB* test lab was entirely unable to cope with the changes to NTFS introduced (although it did offer to create me an 18GB image before crashing out). After a cursory look at a few of the newer commercial imaging systems on the market I quickly decided to hurry along my long-standing plan to switch to a freeware setup, which despite claiming only 'experimental' support for NTFS had no difficulty handling *Vista*.

TEST SETS

The WildList test set was based around the October issue of the list, as the latest available at the deadline set. With few additions in the September list, I had expected a quiet month, but the October list included a bumper 52 new arrivals. In addition to the anticipated wealth of worms and bots, dominated as usual by yet more W32/Mytob varieties and a further glut of W32/Stration, were a handful of W32/Looked samples, more of the file infectors which caused some trouble for a few products a couple of months ago.

The zoo test sets are due for some reorganization and remodelling, but unfortunately there was not enough time to get started on that project before this comparative. Instead, I focused on the set used for testing false positives and speed, which has been the cause of a few issues recently.

The existing set is fairly simple, made up of executables and OLE2 office documents, the same in zipped form, and a handful of dynamically compressed executables held separately. The set has been built up over some time, from various sources, with little evidence of identity or origin attached to the files. While the set makes a useful false positive test, containing numerous strange and wonderful items which have shown themselves capable of tripping up

On-access tests	ItW		Macro		Polymorphic		File infector		Clean set	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	False positives	Susp.
Alwil avast! Home/Professional Edition	0	100.00%	18	98.56%	384	88.22%	33	98.34%	0	1
CA Anti-Virus	0	100.00%	0	100.00%	103	94.39%	3	99.86%	0	0
CA eTrust Integrated Threat Management Suite	0	100.00%	12	99.82%	103	94.39%	3	99.86%	0	0
CAT Quick Heal AntiVirus Plus 2007	0	100.00%	73	98.23%	597	86.06%	151	93.10%	0	0
ESET NOD32 antivirus system	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0
F-Secure Anti-Virus for Vista 2007	0	100.00%	0	100.00%	0	100.00%	3	99.85%	0	0
GDATA AntiVirusKit 2007	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	1
Grisoft AVG	0	100.00%	0	100.00%	302	85.84%	22	96.60%	0	0
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	2	99.88%	0	0
McAfee VirusScan Enterprise	2	99.75%	0	100.00%	46	99.02%	0	100.00%	0	0
Microsoft Windows Live OneCare	37	99.91%	0	100.00%	30	98.11%	12	99.37%	0	0
Norman Virus Control	7	99.12%	0	100.00%	309	99.09%	12	99.43%	1	0
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	14	99.33%	0	0
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0

the best of products from time to time, it is perhaps not the best choice for measuring product speeds. The new set, compiled entirely from scratch, is designed specifically as a speed test rather than aiming to cause false positives; although it is still a subset of the 'clean' collection, and any alerts generated on it will be counted as such during VB100 certification, the files are all fairly ordinary and not expected to surprise any product.

Harvested from a variety of recent *Windows* installations, the set is subdivided into several categories. The 'Executables and System Files' set contains the main bulk, with a large set of executables, both files included with many versions of *Windows* and those associated with a selection of common applications. There are also a large number of DLL library files, and other types of executable, script files, ActiveX controls, drivers and the like.

'Archives' contains a variety of archive formats, mostly the ubiquitous ZIPs but also rar, ace and other compression types, *Microsoft Cabinet* files, and software installers, mostly in *Microsoft Installer* and self-extracting exe format. Other types, such as tar, gz and tgz, are not yet included, but will be added in time for the comparative review of *Linux* products scheduled for two months' time.

'Media and Documents' is made up of most of the common media types found on the average person's home computer: video files in mpeg, avi, wmv and other forms; pictures in common formats such as jpeg, gif and bmp as well as other less popular ones; music and sounds in MP3, wma and other encoding types; web display types including HTML, XML, and Flash animations; and documents, containing not only an array of standard *Office* files (*Word*, *Excel* and *PowerPoint* documents, *Access* databases, *Visio* diagrams), but also PDF files and a stash of simpler data storage formats, csv, rtf and plain old text.

Finally, the 'Miscellaneous' set includes all kinds of other file types, including the mysterious Files With No Extension.

In addition to this new collection of files, the measurement protocol has been adjusted to fit. With the addition of numerous new file types, the issue of which files are scanned becomes more significant. As some products ignore certain filetypes by default, particularly archives, a measure of their throughput in default mode becomes somewhat misleading when compared to another product scanning all files. To avoid this unfairness, the test scan is run twice, once with the default settings and once, in a sharp break from traditional *VB* methods, with the settings changed where necessary to include all files, including looking inside archive files where possible.

Also, on-access scanning speed is now measured, again in both default and full modes where appropriate, as this is widely felt to be a more significant factor from the user's point of view; while on-demand scans can be run at

On-demand tests	ItW		Macro		Polymorphic		File infector		Clean set	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	False positives	Susp.
Alwil avast! Home/Professional Edition	0	100.00%	18	98.56%	384	88.22%	33	98.34%	0	1
CA Anti-Virus	0	100.00%	0	100.00%	103	94.39%	1	99.96%	0	0
CA eTrust Integrated Threat Management Suite	0	100.00%	12	99.82%	103	94.39%	1	99.96%	0	0
CAT Quick Heal AntiVirus Plus 2007	0	100.00%	73	98.23%	597	86.06%	99	96.71%	0	0
ESET NOD32 antivirus system	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0
F-Secure Anti-Virus for Vista 2007	0	100.00%	0	100.00%	0	100.00%	2	99.88%	0	0
GDATA AntiVirusKit 2007	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	1
Grisoft AVG	0	100.00%	0	100.00%	302	85.84%	17	99.02%	0	0
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0
McAfee VirusScan Enterprise	2	99.75%	0	100.00%	46	99.02%	0	100.00%	0	0
Microsoft Windows Live OneCare	37	99.91%	0	100.00%	30	98.11%	9	99.68%	0	0
Norman Virus Control	0	100.00%	0	100.00%	309	99.09%	10	99.57%	1	0
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	12	99.45%	0	2
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	0

off-peak times, on-access slowdown affects users at all times. To measure this, the standard on-access tool is used, which traverses the file structure of the clean test set performing a simple open and close action on each file encountered. The time taken to carry this out is then measured, and compared to the time taken to do the same thing with no on-access protection in place, to produce a rough guide to the on-access overhead.

It is hoped that these changes and new tests will provide a more useful and complete overview of how products perform in a situation more closely resembling the real world. The sets are still in the early stages of development, and any suggestions or queries as to their contents, subdivision or implementation are most welcome.

Alwil avast! 4.7 Home/Professional Edition

ItW	100.00%	**Macro**	98.56%
ItW (o/a)	100.00%	**Macro (o/a)**	98.56%
Polymorphic	88.22%	**File infector**	98.34%

I should perhaps start by saying, by way of excuse, that the products were not necessarily tested in the order in which they are presented here, and my thoughts may appear a little out of joint as a result. The main reason for this was *Alwil* coming so early in the alphabet; I couldn't face starting what I expected to be a difficult and complex batch of tests with a product which I knew was likely to cause difficulties. *avast!*'s on-access behaviour has never failed to baffle me, and its oddities cropped up once again in its *Vista* offering, but happily far less than I expected. Nevertheless, due to the product's strange strategies on access, the accuracy of some of the speed measurements may be a little misleading.

The super-simplified basic interface of *avast!* looks good and may well be fairly easy to use with some practice, but as ever allowed too little fine tuning to be of much use in many of the tests. The speed tests were completed with some ease, and files certainly seemed to be being processed in the on-access mode; on-demand scanning of the WildList and other infected sets was also simple and impressively speedy once I had refamiliarised myself with the complex and fiddly 'advanced' interface.

The changing of settings required much designing and creating of new 'tasks', including a copy of the 'Resident Protection' on-access scanner. On-access detection, the bane of many a previous outing with *avast!*, again had my eyebrows buried in my hairline, as numerous alert messages scrolled up the lower corner of the screen, but little blocking seemed to occur. As far as I can tell, documents and script-type files like VBS/Loveletter were mostly blocked

when opened with my usual utility, while executables were mostly allowed through.

Resorting to copying files onto the machine across the network brought the sought-after happier results, although the logging of detections seemed entirely ineffective, despite the option for such logging being firmly checked. After several passes through the scanner, a check of remaining files revealed nothing of importance left behind, and without false positives aside from a single 'joke' in the clean set, *avast!* is the first product to qualify for the new-look VB100 award.

CA Anti-Virus 8.2.0.13

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	94.39%	**File infector**	99.96%

CA's developers seem determined to keep me busy. For some time, *VB* comparatives have measured the performance of the two engines supplied with the *eTrust* product, with only the default *Vet* option qualifying for the VB100 award. This continued until the last set of tests, when the old *InoculateIT* engine was omitted due to time constraints. Now that it has finally been retired from the product, *CA* has found another way of lengthening my working days – by submitting both its home and corporate products for testing.

The home product was fairly typical of the genre, with much attention paid to attractive styling, in keeping with *Vista* itself. The installer seemed to take some time pondering its surroundings, before shutting itself down, unhappy that the admin user was also logged onto the machine. With this rectified, installation proceeded fairly simply, apart from *CA*'s old trick of forcing the user to scroll through the EULA before it can be acknowledged, as if they'd actually read it. The product itself included various anti-spyware, anti-spam and firewall modules alongside the anti-virus under test, which was somewhat limited as to configuration options.

Speed tests were performed in the default mode only, as I could find no way of changing the settings for scanning file and archive types. It certainly seemed to be paying plenty of attention to the archive files on demand, at one point lingering so long over a particularly large installer that I impatiently rebooted and restarted the test. This second attempt proved more fruitful, getting through the file without further snagging, and scans of the infected sets showed good solid detection, perfectly adequate to earn the VB100 award.

CA eTrust Integrated Threat Management Suite r.8.1

ItW	100.00%	**Macro**	99.82%
ItW (o/a)	100.00%	**Macro (o/a)**	99.82%
Polymorphic	94.39%	**File infector**	99.96%

This new version of *eTrust* seems but little changed from previous editions. Installation followed the old pattern, with the blue-ish grey scheme suitably pastelly in the new environment of *Vista*.

The main interface of the product, a Java thing displayed in a browser, has frustrated me considerably in the past with its slow reaction times, but this updated version showed no such tardiness– the progress bar I have spent many a long hour staring at was barely in evidence this time around. Some of the interface seemed different from my recollection, but not hugely so – perhaps a few new option boxes dropped in here and there. The drop-down for which engine to use is still in evidence, but is now populated only by the *Vet* option, with *InoculateIT* no more than a fast-fading memory.

Again, there was no clear way to tweak scanning settings, and zips seemed not to be scanned internally on access, but speeds in general were highly impressive, and detection good, although a handful of macro samples caught by the home version above were mysteriously missed by its big sister. These were not in the WildList set however, and without a whisper of a false positive, *eTrust* gains another VB100 award.

CAT Quick Heal AntiVirus Plus 2007 version 9.00

ItW	100.00%	**Macro**	98.23%
ItW (o/a)	100.00%	**Macro (o/a)**	98.23%
Polymorphic	86.06%	**File infector**	96.71%

Those wishing to install *Quick Heal* are advised to use the 'Run as Administrator' option, and also to run several of the component files with elevated privileges when required. This certainly seems necessary, as often when omitting these steps the options sections were inaccessible, or other oddities occurred. A few times after a reboot, access to the product, and even apparently on-access scanning, was prevented by *Windows Defender* – it also seemed to be blocking several *Windows* functions from operating, rather oddly.

Using great caution, I coaxed the product through some speed tests. There seemed to be no option to scan all files,

On-demand throughput	Executables and system files				Archive files				Media and documents				Other file types			
	Default		All files		Default		All files		Default		All files		Default		All files	
	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)	Time (s)	Throughput (KB/s)
Alwil avast! Home/ Professional Edition	86	16064.60	128	10793.40	3	225723.31	117	5787.78	19	54854.55	54	19300.68	4	73293.35	5	58634.68
CA Anti-Virus	106	13033.55	106	13033.55	131	5169.24	131	5169.24	90	11580.41	90	11580.41	11	26652.13	11	26652.13
CA eTrust Integrated Threat Management Suite	36	38376.55	42	32894.19	109	6212.57	181	3741.27	14	74445.46	71	14679.39	3	97724.46	5	58634.68
CAT Quick Heal AntiVirus Plus 2007	131	10546.23	126	10964.73	126	5374.36	244	2775.29	52	20043.01	392	2658.77	8	36646.67	20	14658.67
ESET NOD32 antivirus system	32	43173.62	37	37339.35	2	338584.96	161	4206.02	18	57902.03	62	16810.27	3	97724.46	3	97724.46
Fortinet FortiClient	198	6977.55	198	6977.55	168	4030.77	168	4030.77	32	32569.89	32	32569.89	5	58634.68	5	58634.68
F-Secure Anti-Virus for Vista 2007	181	7632.91	190	7271.35	771	878.30	788	859.35	107	9740.53	122	8542.92	12	24431.12	16	18323.34
GDATA AntiVirusKit 2007	205	6739.30	212	6516.77	435	1556.71	506	1338.28	506	2059.76	515	2023.76	13	22551.80	14	20940.96
Grisoft AVG	175.8	7858.68	189.1	7305.95	323.4	2093.91	457.4	1480.48	40.8	25545.01	49.6	21012.83	9.9	29613.47	23.8	12318.21
Kaspersky Anti-Virus	114	12118.91	114	12118.91	367	1845.15	367	1845.15	124	8405.13	124	8405.13	9	32574.82	9	32574.82
McAfee VirusScan Enterprise	119	11609.71	119	11609.71	12	56430.83	178	3804.33	9	115804.06	36	28951.01	8	36646.67	10	29317.34
Microsoft Windows Live OneCare	88	15699.50	88	15699.50	476	1422.63	476	1422.63	97	10744.71	97	10744.71	9	32574.82	9	32574.82
Norman Virus Control	444	3111.61	444	3111.61	94	7203.94	94	7203.94	16	65139.78	16	65139.78	24	12215.56	24	12215.56
Sophos Anti-Virus	218	6337.41	226	6113.08	16	42323.12	194	3490.57	38	27427.28	177	5888.34	12	24431.12	20	14658.67
Symantec AntiVirus	95	14542.69	95	14542.69	131	5169.24	131	5169.24	31	33620.53	31	33620.53	10	29317.34	10	29317.34

but further types could be added manually to the rather sparse extension list, and even with standard settings speed was a little below my expectations from previous experiences with *CAT* products. Running over the infected sets, at first I foolishly omitted to deactivate the warning popups for the on-access mode, causing a barrage of alerts one on top of another which, when I returned to the machine some time later, had frozen it completely. A message warning me my performance seemed to be falling sat forlornly beneath the paralysed mouse cursor. After a reboot and a tweak to the settings, the test was run with more success, and results showed a few misses in the zoo but nothing in the wild, with no false positives; a VB100 award goes to *CAT*.

ESET NOD32 antivirus system 2.7

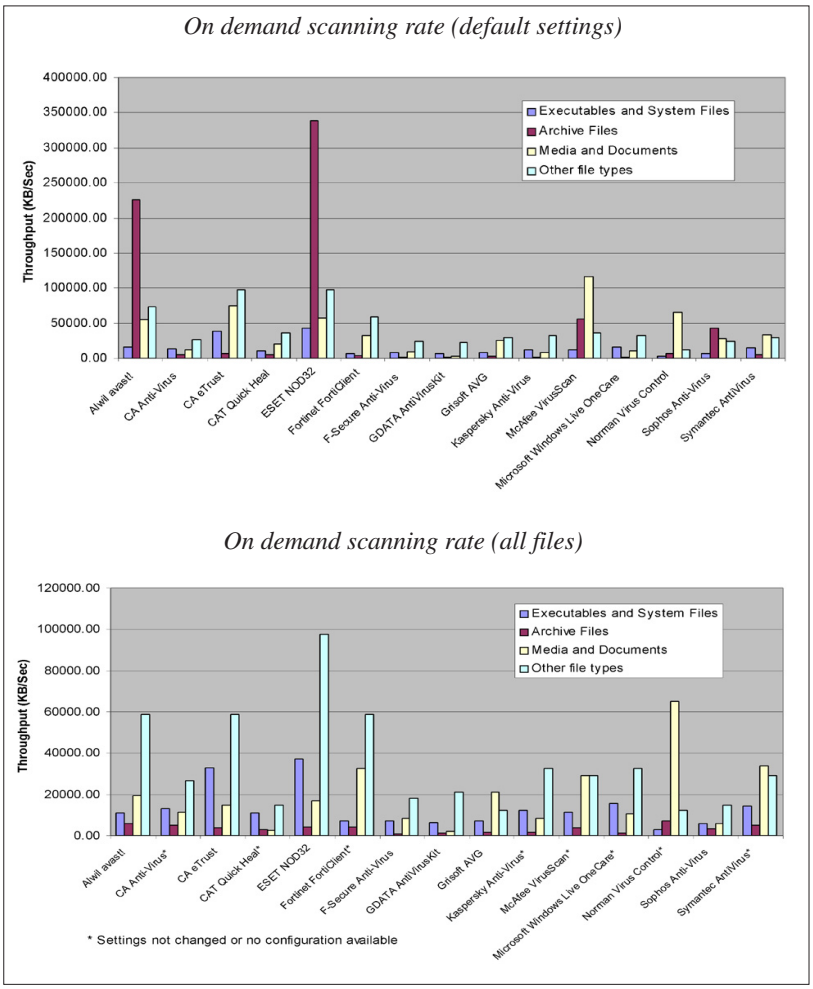
ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	100.00%	**File infector**	100.00%

The grey of *NOD32*'s installation procedure suddenly looked rather dowdy and old-fashioned when surrounded by the flashy, colourful window borders provided by *Vista*. Somehow, however, despite the very un-*Vista*-like styling, the control centre maintained an air of aloof futuristic power with its separable windows, and some pleasantly fast-opening tooltips helped identify the modules otherwise only known by codewords. AMON zipped through the on-access speed tests, while the *NOD32* scanner, looking very glossy in its stylish new window, was its usual pacey self in the on-demand tests.

I had quite forgotten that acquiring logs requires some rather unintuitive behaviour, opening the log in a viewer, selecting an individual entry, right-clicking and selecting export to drop the data into a parsable file. The log viewer had some scrolling issues, with the horizontal scroll bar disappearing before I could see the end of lines, and another problem arose when trying to open the on-access log from the infected files test; the product seemed to freeze entirely, although it is of course enormously unlikely that anyone outside a test lab would ever have so many detections on access all at once. Fortunately, I didn't really need this log to complete my analysis of results, which as expected proved excellent. Not a single miss or false positive gives *ESET* another VB100 award, and the ever-impressive speed was barely affected by the addition of archives for the on-demand test.

Fortinet FortiClient 5.0.379

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	100.00%	**File infector**	100.00%



F-Secure Anti-Virus for Vista 7.00

ItW	100.00%
Macro	100.00%
ItW (o/a)	100.00%
Macro (o/a)	100.00%
Polymorphic	100.00%
File infector	99.88%

F-Secure's *Vista* product was still in Beta at the time of submission for the test, freely downloadable for trial purposes. Installation, featuring *F-Secure*'s current colour scheme of flat, brilliant whites and cool blues, looked a little odd inside the more shimmery stylings of *Vista*, but functioned perfectly well, demanding an administrator log in after an initial reboot to 'complete the installation.' Unfortunately, it was unable to call home from my lab to 'validate' itself, and I was warned I only had seven days to complete my tests before it deactivated.

Fortunately, this proved just about enough time. The controls were familiar from previous versions, but I frequently found myself disconcerted by the greying-out of options in the configuration dialogues, and confused by the need to use the 'change' option before the 'configure' option had much power.

Speeds were decent in most of the tests, with extending the range and depth of scanning making little difference in the archive set scanning time on demand; on access, however, it was quite another story, with extensive examination slowing things to a snail's pace, proving that *F-Secure* developers were quite right to switch this off by default.

The scanning of large numbers of infected files was equally sluggish, and the log wizard displayed some bizarre behaviour when asked to show me details of a sizeable scan, popping up a pretty HTML log with a small subset of the detection, which varied wildly in size each time I clicked the button. Clearly, this sort of user-friendly wizard is not designed for such unusually large files, and a simpler version of the log was obtained easily for checking.

Some excellent scores, with only a few samples missed among the file types that the product deliberately avoids in default mode, more than made up for the extra time taken. *F-Secure* wins the VB100 award with some ease.

Fortinet's *FortiClient* is a pretty complete product, with a broad range of features offered by the array of tabs for its various functions lined up down the side. As such, it was little surprise that during the installation, aside from requiring the administrator password at the start, the installation of no less than three drivers had to be confirmed as expected behaviour.

Once set up, the GUI looked much as ever – serious and option-rich, although the tone was lightened somewhat by the bright shiny outline provided by *Vista*.

Scanning over the various speed tests was reliable and impressively pacey. *FortiClient* was one of very few products in this test to scan all files by default both on demand and on access. Detection was similarly excellent, with the few misses in the zoo sets seen in the last couple of *VB* comparative reviews eradicated. Without false positives either, *FortiClient* once again earns its VB100 award comfortably.

On-access slowdown	Executables and system files				Archive files				Media and documents				Other file types			
	Default		All files		Default		All files		Default		All files		Default		All files	
	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)	Time (s)	Slowdown (%)
Alwil avast! Home/ Professional Edition	12.587	513.60%	16.562	707.38%	1.312	1493.52%	3.859	4587.04%	17.546	3051.98%	24.393	4281.98%	1.609	259.42%	2.203	392.11%
CA Anti-Virus	96.656	4611.86%	96.656	4611.86%	5.796	6939.68%	5.796	6939.68%	34.406	6080.72%	34.406	6080.72%	10.843	2322.11%	10.843	2322.11%
CA eTrust Integrated Threat Management Suite	37.734	1739.49%	38.102	1757.43%	4.187	4985.43%	4.238	5047.37%	15.703	2720.90%	15.873	2751.44%	4.5	905.21%	4.863	986.30%
CAT Quick Heal AntiVirus Plus 2007	164.093	7899.33%	164.093	7899.33%	120	145648.99%	120	145648.99%	35.523	6281.38%	35.523	6281.38%	3.234	622.41%	3.234	622.41%
ESET NOD32 antivirus sytem	42.671	1980.16%	42.671	1980.16%	3.265	3865.59%	3.265	3865.59%	22.87	4008.38%	22.87	4008.38%	4.328	866.79%	4.328	866.79%
Fortinet FortiClient	202.375	9765.53%	202.375	9765.53%	51.25	62146.96%	51.25	62146.96%	31.203	5505.33%	31.203	5505.33%	8.062	1700.89%	8.062	1700.89%
F-Secure Anti-Virus for Vista 2007	182.78	8810.30%	267.435	12937.13%	6.265	7509.31%	2023.043	2457037.25%	28.758	5066.11%	182.867	32750.36%	6.875	1435.74%	27.39	6018.39%
GDATA AntiVirusKit 2007	155.921	7500.96%	164.113	7900.31%	11.453	13810.53%	420.313	510401.62%	162.796	29144.79%	122.542	21913.53%	26.206	5753.91%	26.234	5760.16%
Grisoft AVG	135.359	6498.59%	136.843	6570.93%	2.812	3315.38%	4.5	5365.59%	32.875	5805.69%	40.8	7229.34%	2.984	566.57%	4.203	838.87%
Kaspersky Anti-Virus	16.39	698.99%	100.609	4804.57%	0.656	696.76%	5.734	6864.37%	5.234	840.24%	24.781	4351.68%	7	1463.66%	10.39	2220.92%
McAfee VirusScan Enterprise	116.437	5576.16%	115.031	5507.62%	9.859	11874.49%	171.14	207762.35%	21.515	3764.97%	32.781	5788.80%	5.843	1205.21%	8.187	1728.82%
Microsoft Windows Live OneCare	71.75	3397.73%	71.75	3397.73%	9.078	10925.91%	9.078	10925.91%	45.417	8058.74%	45.417	8058.74%	6.625	1379.90%	6.625	1379.90%
Norman Virus Control	48.937	2285.62%	48.937	2285.62%	2.218	2593.93%	2.453	2879.35%	15.265	2642.22%	15.33	2653.89%	8.363	1768.13%	8.578	1816.16%
Sophos Anti-Virus	180.468	8697.60%	200.062	9652.78%	8.5	10223.89%	169.515	205788.66%	34.375	6075.15%	167.335	29960.18%	34.375	7578.70%	8.906	1889.43%
Symantec AntiVirus	74.627	3537.98%	74.627	3537.98%	4.468	5326.72%	4.468	5326.72%	12.796	2198.68%	12.796	2198.68%	5.156	1051.75%	5.156	1051.75%

G-DATA AntiVirusKit 2007 17.0.6353

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	100.00%	**File infector**	100.00%

G-DATA's *AntiVirusKit* has had a glossy redesign fairly recently, with its twinkly badges, fading colours and fancy icons sitting comfortably amongst the equally fancy *Vista* themes. Installation demanded logging in fully as the admin user, rather than just a confirming password, but once installed protection could be disabled by a standard user without prompting.

One of few products in this review to combine the efforts of two separate scanning engines, speeds were still reasonable, and despite a stern warning when I disabled the size limit on archive files, that it could seriously slow down my system, the overhead was not too great. Intensive scanning inside CHM files seemed to lengthen the time on the media set, but this was not extended much by adding further depth.

The usual excellent results were obtained over the infected sets, with the doubled engine ensuring complete coverage of all sets. But just as I was starting to think everyone would be passing cleanly this month, the ball was dropped; a false positive in the clean set, and another on the same file in zip format on demand, denies *G-DATA* a VB100 award this time.

Grisoft AVG 7.5.433

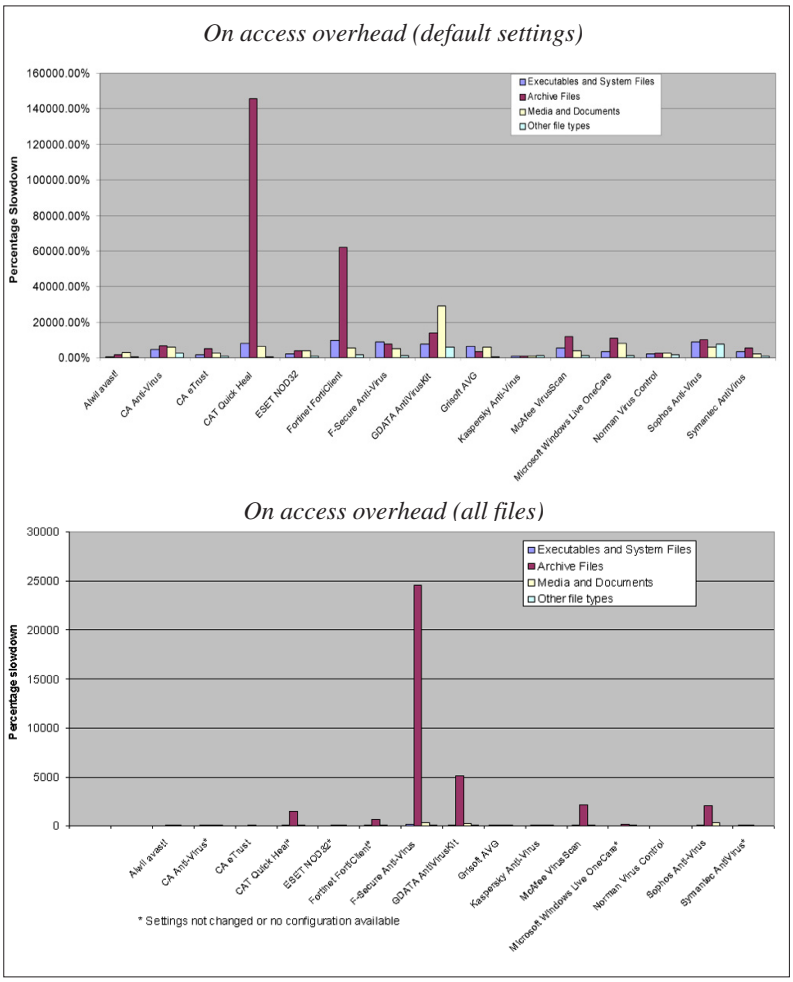
ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	85.84%	**File infector**	99.02%

AVG's installer is a bare and simple thing, featuring some large and sparse artwork of folders and other computery things, with a single request for the administrator password and no reboot required.

The product itself was less straightforward, at least in the 'Advanced' mode required for my testing, with a wealth of windows appearing to control various tasks and options. An information page told me, rather cutely, that I was running 'Windows Longhorn Professional', which was the early codename for *Vista*.

While the styling remains simple, the convoluted design of *AVG*'s controls had me baffled a few times, before calm and sober pondering of the menus led to the required dialogue. With the GUI's code cracked, tests were carried out fairly easily, with the speed tests looking fairly decent and coverage of viruses also reasonable.

With a fair chunk of the older polymorphics and file infectors missed, but nothing significant elsewhere, *AVG* can add another VB100 award to its set.



Kaspersky Anti-Virus 6 Beta 6.0.2.546

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	100.00%	**File infector**	100.00%

Kaspersky's product, in Beta at the time of testing, also maintains the design and styling of previous versions; the familiar green and red of the installer provided some simple options, and required the admin password to complete. Applying updates was a little more troublesome, with the product taking some time to register a change of source; after removing the default and adding a network folder as its target, it persisted in trying to contact an ftp server somewhere in Europe for some time, before eventually registering the change and finding the correct update sources.

Once this was done, no further problems were encountered, with the interface providing all the options I needed quite easily, and scanning proceeding in a fairly rapid and thorough fashion. This was another product to allow deactivation of its monitors by a standard user.

On demand, the product defaults to scanning all files, although archives are normally missed on access, accounting for the unusual speed over the archive set. To achieve full scanning, an option to scan all files rather than only selected types was set, as were further check boxes for archives and installers, and the slowdown thus caused brought speeds down to more normal, but certainly not slow, levels.

As far as certification goes, *Kaspersky* reached the necessary standard with ease once more, with the only misses caused by not scanning zip files by default, and as a result *Kaspersky* is awarded another VB100.

McAfee VirusScan Enterprise version 8.5i

ItW	99.75%
Macro	100.00%
ItW (o/a)	99.75%
Macro (o/a)	100.00%
Polymorphic	99.02%
File infector	100.00%

McAfee's latest product is also little changed to the naked eye, with just a few beautifications here and there. The installer spent some time pondering its new surroundings before getting going, but once off the mark got things set up fairly speedily, with no need for a reboot to get itself active. Some aspects of the GUI were a little fiddly, with some of the deactivation controls greyed out but available as options on the system tray icon.

Opening the console, like a few of the other products, required confirmation of my possibly dangerous actions, which makes the screen behind fade out, and a few times on clicking the 'reset to defaults' button on a configuration page, a similar effect occurred, leading me to think I had crashed out the console. However, all it needed was to close itself down and restart to apply the changes, and all was functional once more.

Speeds were pretty good, and the configuration logical and easy to follow; scanning over most of the test sets was fairly solid too, but both on access and on demand the product committed the ultimate sin and missed WildList viruses, thus spoiling *McAfee*'s chances of a VB100 award on this occasion.

Microsoft Windows Live OneCare 1.5

ItW	99.91%	**Macro**	100.00%
ItW (o/a)	99.91%	**Macro (o/a)**	100.00%
Polymorphic	98.11%	**File infector**	99.68%

This was my first experience of the *Microsoft* product, which is already in its second incarnation. Long amused by the name, which in the kindest light is reminiscent of a famous chocolate factory owner, I had been looking forward to trying it out for some time, and was almost denied the opportunity by a series of snags. The original submission was no more than a downloader, requiring Internet access to retrieve the bulk of the software. Some rapid explanation of the sealed-off nature of the *VB* lab brought a special version with some adjustments to the setup allowing it to be installed offline, which for a while sat untouched on the test bench, awaiting its turn. When I finally tried to get it going, the installer failed halfway through – a problem, I was told, due to access rights; running it as administrator got me slightly further, but in the end the UAC had to be completely disabled to get things up and running. I assume these steps are not necessary with the proper online installation process.

One look at the GUI lengthened my face considerably. There were not a lot of controls here, no tabs full of sliders and check boxes, no 'advanced mode' button for the serious user. My first glance at the settings page showed very few options indeed – 'On' and 'Off' seemed to be the extent of it, although closer examination revealed options to exclude certain files and areas, and also to inspect the quarantine area. A log was also available, which again I did not spot at first.

Looking back at *OneCare*'s only previous appearance in a *VB* comparative (see *VB*, June 2006, p.11), I see my predecessor had similar problems, describing the product as 'a paranoid nanny'. His experiences back then were again mirrored after the on-access test, when the product ground to a halt, its interface fading to a pale pink with the ever-comforting '(Not responding)' appearing in the title bar. Even a reboot failed to solve this problem, and I ended up reimaging the machine and starting from scratch, although fortunately the results of the on-access scan, and some of the speed tests, were safely in. Again, I would assume that the unusual situation (the improbably large number of detections encountered in a short period) is probably at the root of this problem.

On-demand scans were similarly tricky. While the speed tests were fairly easy, producing good results, of course without the ability to change the settings it was difficult to tell how much scanning was going on; archives were clearly being delved into to some extent, on demand at least.

Scanning the virus collections seemed to be going well, until the auto-cleaning began bludgeoning its way through the system32 folder to check for real infections. I began my first attempt mid-afternoon, and watched it climb fairly rapidly to 90%, where it remained for several hours and it was still hovering there when I returned next morning.

Another try at this finally got it through, and after getting some advice on acquiring logs for parsing, I finally got some results. The log contained a number of error messages for files in the system folder that had proved unscannable, in part explaining the trouble with completing the cleaning process. Detection of viruses, on the other hand, was generally decent, with a small handful of misses in the zoo sets, but more significantly numerous samples of one of the W32/Looked variants in the WildList set were missed in both modes, and so *OneCare* misses out on a VB100 award for now.

Norman Virus Control version 5.90

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	99.12%	**Macro (o/a)**	100.00%
Polymorphic	99.09%	**File infector**	99.57%

Norman was again little changed from the user angle, a situation which disappointed me somewhat as I've always found the interface a little awkward. Installation was straightforward, with full admin login required but no extra demands for confirmation, and no reboot was called for; it seems to be required however, as at first the product exhibited some unusual behaviour, not least having no icon in the system tray from which to access the controls easily.

Restarting the machine rectified this and the scanning oddities, and testing proceeded, slowed only by the complicated and window-heavy task of setting up and running scan tasks. Speeds were more impressive on access, even with more complete settings switched on, than on demand, in which mode all files are scanned by default, although internal scanning of archives seemed to be eschewed at all times, with no option to enable such in-depth analysis.

On demand, *Norman*'s usual handful of misses in the zoo sets were unsurprising, but a trojan detected in the clean test set complicated issues somewhat; the file in question was the installer for a competitor's anti-rootkit product, the inclusion of which in the test set was made after some thought as to its appropriateness. The issue of failing a product after tricking it with a file known to be difficult became irrelevant, however, when several ItW viruses, which had been detected with ease on demand, were missed repeatedly on access, and *Norman* misses out on another VB100 award.

Sophos Anti-Virus version 6.5.1

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	99.80%
Polymorphic	100.00%	**File infector**	99.45%

After several days awash in this sea of troubles, reaching the *Sophos* product was like the reassuring crunch of a sandy beach beneath the fast-eroding bit of driftwood that is my mind, with firm trees laden with plump fruit on the skyline. Suddenly it was as if *Vista* had never happened; *Sophos*'s installer and components looked and felt just like they have done in the last half-dozen tests, since the last major redesign of the product a year or two ago.

Sophos made much, during the recent brouhaha over access to details of the inner workings of *Vista*, of how well prepared its developers have been for the launch, and playing briefly with this version shows the boasts were pretty justified. Installation was fast and slick, with just the one standard request for admin rights, and once installed the controls seemed properly suited to the UAC, with most configuration options blocked for the normal user and accessible only to the administrator. The GUI remains unchanged, not beautiful but functional, with not a cunningly hidden option to be rummaged for, and at last I had found a product where everything seemed just to work.

Speeds were pretty decent, and detection hit the usual solid levels, with a few file types and obscure older samples avoided. In the clean set a couple of files, both process manipulation utilities from *SysInternals*, were labelled as potential hacking tools, but as such definitions are allowed within the rules, *Sophos* earns a VB100 award, and a sigh of grateful relief from me.

Symantec AntiVirus 10.2.0.276

ItW	100.00%	**Macro**	100.00%
ItW (o/a)	100.00%	**Macro (o/a)**	100.00%
Polymorphic	100.00%	**File infector**	100.00%

Symantec has yet another installation process that demands full administrator rights, but after a few false starts even this was not enough. Following some slightly inaccurate instructions in the readme, I changed some security settings in various MMC plugins, which enabled installation to proceed, disabling *Windows Defender* along the way, I noted.

Once set up, the product produced no further problems, with the normal GUI looking as serious and sensible as ever, wordy and adorned only with small, sober icons.

Configuration was fairly straightforward, although I could find no option to scan zips internally on access for the new speed tests, making the speeds look even more impressive than they perhaps should, and detection across all sets was impeccable. Without false positives either, Symantec also earns another VB100 award.

CONCLUSIONS

As expected, the combination of *Windows Vista* and a set of new tests proved a tricky one. The operating system itself gave me few problems – although I managed to induce a blue screen within a minute of my first install, this proved to be an isolated incident. The new styling I often found a little garish, and the prettified behaviour of various buttons and menus a trifle fiddly, but I managed to resist the temptation to revert to the 'classic' theme in order to appreciate the products under test against the very latest backdrops.

Many of the products, however, presented more serious problems, with numerous freezes, crashes and freakings-out to be contended with. Some required lots of coaxing to avoid the UAC controls, others had more serious problems with sections apparently not functioning at all. A select few managed to handle the new environment with ease.

On the detection front, false positives were perhaps fewer than normal, despite some enlargement of the clean set made in conjunction with the creation of the speed set, but misses of WildList samples were quite high, with three products missing more than one sample (although one missed numerous samples of a single, rather prolific, virus). At least one of these, occurring only in one mode, can perhaps be put down to a problem with integration into the new operating system.

The new speed tests added somewhat to the workload, but it is hoped the data gathered will be of some interest to *VB*'s readers. The addition of more in-depth scanning times for comparison was perhaps less successful than I had hoped, with many products short on configuration options, others less than clear about what was being scanned. The figures are thus presented as a rough guide, and readers should use their own judgement in interpreting them. Work will continue on refining both the test sets and the testing techniques, and any feedback or suggestions will be greatly appreciated.

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 the 32-bit version of *Microsoft Windows Vista, Business Edition*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Vista/2007/test_sets.html.