COMPARATIVE REVIEW

WINDOWS XP SERVICE PACK 3

John Hawes

This month the VB100 test schedule rolled around once again to the *Windows XP* test – which was expected to be the most heavily subscribed of the year. However, a handful of withdrawals and no-shows meant that the crowd of submissions fell mercifully short of the 40 or so it had threatened to reach, but still promised to keep me busy throughout the test period. A new batch of test systems was ordered in time for this review – but unfortunately, half the shipment didn't arrive until well into the testing period, which actually slowed testing down rather than streamlining it. Hoping that most of the products – by now fairly familiar to me – would move on and off the test bench at a reasonable rate, a sprinkling of new names piqued both interest and apprehension, as did news that many of the regulars would be submitting heavily updated or redesigned versions. Some major updates to the zoo test sets, part of an ongoing programme of improvements, also added a new zest to this month's test.

PLATFORM AND TEST SETS

As testing for this comparative got underway, something of a milestone in the history of the *Windows XP* platform was reached – on 30 June, most versions of the operating system ceased to be sold via most OEM and retail channels. Licensing will continue to be available for 'System Builders' until January 2009, and in April official support for the platform will be downgraded to an 'extended' period set to continue until 2014. These first steps towards putting the platform out to pasture seem somewhat premature, given its continuing popularity and massive market penetration.

With its slicker, more advanced successor *Windows Vista* now well past its launch stage and settled in as the default (and in many cases only available) operating system for new PCs, *Windows XP* has maintained its dominance as the platform of choice for the majority of PC users. Looking at a selection of studies of platform usage, *XP*'s figures are declining very slowly, currently estimated as being in use on around 75% of systems while *Vista* has crept up to 15%. Many businesses continue to run *XP* on their workers' desktops, even where this entails removing *Vista* from new purchases. At this rate, *XP* looks set still to be the most widely used *Windows* version when the next new release, the successor to *Vista* currently going by the title 'Windows 7', hits the shelves – currently scheduled for around two years' time.

Adding further to the longevity of *XP* is the latest service pack, released a few months ago and added to the Automatic Update system during July. The update contains a number of new features, many of which are related to security, authentication and encryption, but for the majority of users is expected to make little obvious impact. In the weeks following initial release of the service pack, a number of issues were spotted arising from clashes between various aspects of the update and a selection of third-party anti-malware and security products, but most were quickly resolved. This test should see products at the top of their game, on a mature and stable platform, but as usual there is no knowing just how the range of updates will affect the products during the in-depth grilling applied on the *VB* test bench.

The toughness of this month's test was kept to a minimum thanks to an early deadline (intended to allow adequate time to deal with the anticipated glut of entries), which meant that the release of the May 2008 WildList narrowly missed the cut-off date for this month's test. The test sets were frozen on 20 June, using the April WildList for the core certification set, with the product submissions taken and frozen on 24 June.

The false positive set saw its usual expansion with new files and packages, and the other test sets were also extended somewhat, most notably the polymorphic set which saw several new items introduced in fairly limited numbers. This will be added to over the next few months as further generations of samples are replicated and verified.

The legacy set of older and more obscure items was left out of this test, something which has been planned for some time. Interest in such items continues to fluctuate, with a surprising number of macro and even DOS viruses still cropping up on the prevalence reports we gather, and this set may occasionally be resurrected for server tests where it has more relevance. In its place is a new set of trojans, an introductory selection of several thousand samples gathered over the course of the last six months or so. This move heralds a planned expansion in this direction for the *VB* sets, and we hope to have further improvements in the upcoming tests.

With an entirely new set of samples to measure detection against, a new platform on new hardware and a selection of new products, I expected the month of testing to be eventful, so I quickly got down to the lab and started testing.

Agnitum Outpost Security Suite Pro 6.0.2296.253.0490

ItW	100.00%	**Polymorphic**	77.32%
ItW (o/a)	100.00%	**Trojans**	84.22%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Agnitum's suite was reviewed in depth a few months ago (see *VB*, January 2008, p.17) and remains little changed on the surface. The installation process is rather protracted, both in terms of the selections required of the user and in the time taken to perform the installation, with a reboot required at the end to get things going. The complexity of the installation process is explained by the wide range of security extras, in particular the firewall for which *Agnitum* is renowned. The anti-malware component, supported by the *VirusBuster* scanning engine, receives minimal attention in the interface design. Configuration is fairly limited, particularly for the on-access scanner, and the layout of the manual scanning system a little fiddly, but the default setup and the few available options proved ample for most of my needs.

The product ran smoothly and with rock-solid stability, racking up some reasonable if not superb scanning speeds, decent coverage of the trojan test set and no issues at all in the WildList or clean sets, thus easily qualifying for a VB100 award.

Ahnlab V3 Internet Security 7.0 Platinum Enterprise 7.6.3.1

ItW	99.99%	**Polymorphic**	92.86%
ItW (o/a)	N/A	**Trojans**	84.34%
Worms & bots	99.81%	**File infectors**	97.64%
False positives	0		

Ahnlab's offering is another full suite, boasting a range of modules including anti-virus, anti-spyware, anti-hacking (which comprises a personal firewall and intrusion prevention elements), privacy control and email protection. The setup and installation process is much less complex than might be expected however, with no reboot required, and protection is up and running very quickly. A prompt requesting approval of the activities of svchost.exe pops up even before the installation is complete. Whether such a prompt would help the majority of users, who would be unlikely to understand its implications and may well simply click 'allow' without further thought, is perhaps somewhat questionable, but it does indicate a thoroughness of protection available to those with the understanding to apply it properly.

Configuration was rather limited and the layout a little confusing, with some options held in a central location while others appeared on specific sections for each module, and again the system for setting up a scan was somewhat awkward. Scanning speeds were pretty unexceptionable, but measurements were hampered by several crashes during the running of the speed tests, requiring them to be restarted.

Worse, while running the on-access detection tests the system crashed completely, with the famous blue screen putting in a rare appearance. Several repeat attempts brought similar results. On contacting the developers, it emerged that an engine update may have introduced issues with the handling of polymorphic items, thus causing the crashes. Having been unable to complete the on-access component of the test, *Ahnlab* does not qualify for a VB100 award on this occasion.

Alwil avast! 4.8.1214

ItW	100.00%	**Polymorphic**	88.78%
ItW (o/a)	100.00%	**Trojans**	97.66%
Worms & bots	99.48%	**File infectors**	96.06%
False positives	0		

Alwil's ever-popular *avast!* seemed much the same as ever, although apparently a new suite offering has recently been added to the company's line-up (something I hope to have a closer look at in the near future). For now the traditional design continues to frustrate somewhat while providing ample control and configuration for those who can find it. The installation was simple but required a reboot of the system, with the option to launch a scan immediately on restart.

Default settings are fairly limited in depth, with the on-demand scanner ignoring files with extensions not expected to be used by malware, although the on-access component checks further in depth and was able to spot the EICAR test file despite a random extension. Archives were likewise ignored in the default settings but covered flawlessly when requested. Speeds were splendid, remaining fairly good even with more paranoid settings, and detection rates were also excellent, including very impressive coverage of the new trojan set. With nothing in the WildList set missed and no false positives, *Alwil* adds another VB100 award to its tally.

ArcaBit ArcaVir 08.06.3218.4

ItW	95.80%	**Polymorphic**	94.16%
ItW (o/a)	95.80%	**Trojans**	76.12%
Worms & bots	99.78%	**File infectors**	98.62%
False positives	10		

ArcaBit was unfamiliar to me prior to this review, but it has some history in VB comparative testing with two entries in 2005, coming very close to achieving VB100 certification (see *VB*, February 2005, p.12 and *VB*, June 2005, p.11). The company is based in Warsaw, Poland, and provides a full

On-access detection	WildList		Worms and bots		File infectors		Polymorphic		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.91%	8	99.21%	317	77.32%	347	84.22%		
Ahnlab V3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A		
Alwil avast!	0	100.00%	6	99.48%	6	96.06%	322	88.78%	51	97.66%		
ArcaBit ArcaVir	182	95.80%	3	99.78%	6	98.62%	55	94.16%	525	76.12%	10	2
AVG Internet Security	0	100.00%	1	99.94%	1	99.21%	52	89.95%	58	97.36%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	38	98.27%		
BitDefender AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	116	94.75%	3	
Bullguard	2	99.92%	12	99.22%	2	98.95%	0	100.00%	96	95.62%	2	
CA AntiVirus + AntiSpyware	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
CA eTrust	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
eEye Blink Professional	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	238	89.20%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	92	95.54%	1854	15.73%		
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	0	100.00%	90	95.65%	250	88.63%		
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	30	98.55%	129	94.15%		
F-Secure Protection Services	0	100.00%	0	100.00%	0	100.00%	30	98.55%	129	94.15%		
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	21	99.04%		
K7 Total Security	0	100.00%	5	99.61%	5	97.32%	1072	64.74%	455	79.33%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	30	98.55%	137	93.79%		
Kingsoft Internet Security	0	100.00%	15	98.97%	87	81.89%	2009	42.15%	662	69.91%	1	
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	341	84.52%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	0	100.00%	90	95.65%	106	95.17%		
Norman Security Suite	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
NWI Virus Chaser	12	98.27%	0	100.00%	0	100.00%	90	95.65%	93	95.77%		2
PC Tools AntiVirus	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		
PC Tools Spyware Doctor	0	100.00%	2	99.91%	8	99.21%	313	77.70%	407	81.52%		
Proland Protector Plus	162	99.53%	5	99.48%	59	90.79%	1722	46.38%	1973	10.30%		
Quick Heal AntiVirus	0	100.00%	53	93.15%	10	98.03%	908	81.51%	1465	33.40%		
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	90	95.65%	102	95.38%		
Rising Antivirus	0	100.00%	2	99.81%	41	94.33%	1302	52.19%	292	86.74%		
Sophos Endpoint Security & Control	0	100.00%	0	100.00%	0	100.00%	90	95.65%	46	97.93%		33
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	90	95.65%	38	98.29%		
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	561	87.72%	40	98.20%		
VirusBuster Professional	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		2
Webroot AntiVirus with AntiSpyware	0	100.00%	4	99.48%	0	100.00%	107	95.06%	50	97.75%		

range of products including support for a range of Unix and *Linux* platforms, servers, mobile devices and an online scanner. The product submitted for testing includes a firewall, mail scanning and anti-spam, as well as some extras including registry monitoring, web scanning and a 'Care' module, all of which are disabled in a default installation but can be enabled at will. The setup process is thus rather lengthy, and requires a reboot at the end, but it is clearly laid out and looks very slick and professional.

The product itself is similarly impressive, with a clear and brightly coloured interface which was very easy to navigate. There was an unexpected lag during the setting up of manual scans, with the 'browse' button taking up to a minute to respond and present the filesystem for browsing, but otherwise things went smoothly, with decent scanning times and pretty good detection. This did not quite carry far enough however, as several of the highly complex variants of W32/Virut, which have been causing problems for a wide range of products for some months now, were not fully covered. This skews the results table somewhat, as the seemingly large number of misses in fact only represents a small number of unique viruses, so the percentage is a better indicator of performance than the raw number of missed files.

A smattering of false positives pushed a VB100 award further out of reach this time, but *ArcaBit* seems likely to reach the required standard in the very near future.

AVG Internet Security 8.0.131

ItW	100.00%	**Polymorphic**	89.95%
ItW (o/a)	100.00%	**Trojans**	98.47%
Worms & bots	99.94%	**File infectors**	99.21%
False positives	0		

Another suite, again reviewed in these pages fairly recently (see *VB*, March 2008, p.18), *AVG*'s *Internet Security* offers a splendidly fast and easy installation process, with everything up and running within a couple of minutes with no hard thinking or even a reboot required. Once the initial install is complete, however, a series of further setup phases are necessary, including options to install a *Yahoo!* toolbar and to set the browser to default to using *Yahoo!* for searches, a firewall configuration wizard, and several other steps.

With this stage complete things moved on very quickly, the product providing a clear and logical interface with no surprises. An oddity cropped up in the on-access side of testing, when the option to enable scanning of archives seemed to have little or no effect. Speeds were a little sluggish but detection rates excellent, with very little missed anywhere and no false positives either. With the WildList fully covered, *AVG* picks up another VB100 award.

Avira AntiVir 8.1.0.582

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.27%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

AntiVir presented a similarly straightforward and zippy installation process, again with no reboot and this time with no further requirements of the user. The familiar interface has its quirks but is easily navigated, with a few touches here and there either newly added or simply not noticed before, including some very funky slider controls.

A few times after running speed tests the 'Luke Filewalker' scanner screen seemed to linger rather longer than expected before closing down, but never for more than 10 seconds, and scanning speeds were extremely impressive. Detection rates were even closer to perfection, and without a hint of a false positive, and barely anything missed, *Avira* comfortably wins another VB100 award.

BitDefender AntiVirus 2008 11.0.16

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.75%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	4		

BitDefender's installation process takes a little time, with a blank setup window lingering on screen for 30 seconds or so before things get underway, followed by another lull as the *Windows Installer* prepares itself for action. The standard set of options follows, and once the installer proper is kicked off things move pretty speedily to completion. Prompts to enter a licence code and to reboot the system then appear simultaneously.

After the reboot the interface is simple and straightforward, but plenty of fine-tuning options are available in an advanced configuration area. Initial attempts to run on-demand scans proved a little troublesome, as requests returned strange messages claiming the scan could not be carried out, but a second restart of the system put a stop to these anomalies. From then on testing ran smoothly and quickly, with good scanning speeds and top-notch detection levels. WildList detection was flawless and the other sets not far off, but a small cluster of false positives put paid to *BitDefender*'s hopes of a VB100 award this month.

Bullguard 8.0.0.7

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	99.92%	**Trojans**	95.62%
Worms & bots	100.00%	**File infectors**	98.95%
False positives	4		

The *Bullguard* installation process was snappier, taking little more than a minute all told, with a reboot required at the end. This was followed by a registration process which asked for the user's email address and connected to base to report back – a six-day 'grace period' is allowed where this is not possible.

The interface is very simple and novice-friendly, offering basic controls for anti-virus, anti-spyware and a firewall. Little in-depth configuration was provided, but the defaults seemed sensible and more than adequate for my needs. Speeds and detection rates closely followed the example set by the parent *BitDefender* product, but a couple of misses of samples in the WildList set on access, along with those few false positives were enough to spoil things for *Bullguard* this time round.

On-demand detection	WildList		Worms and bots		File infectors		Polymorphic		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.91%	8	99.21%	317	77.32%	347	84.22%		
Ahnlab V3	2	99.99%	3	99.81%	8	97.64%	526	92.86%	345	84.34%		
Alwil avast!	0	100.00%	6	99.48%	6	96.06%	322	88.78%	51	97.66%		
ArcaBit ArcaVir	182	95.80%	3	99.78%	6	98.62%	55	94.16%	525	76.12%	10	2
AVG Internet Security	0	100.00%	1	99.94%	1	99.21%	52	89.95%	34	98.47%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	38	98.27%		
BitDefender AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	116	94.75%	4	
Bullguard	0	100.00%	0	100.00%	2	98.95%	0	100.00%	96	95.62%	4	
CA AntiVirus + AntiSpyware	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
CA eTrust	0	100.00%	0	100.00%	1	99.84%	96	95.37%	1015	53.86%	1	
eEye Blink Professional	0	100.00%	0	100.00%	7	99.15%	1005	67.12%	145	93.43%		
ESET NOD32 Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	48	97.84%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	92	95.54%	1854	15.73%		
Frisk F-PROT Antivirus	0	100.00%	0	100.00%	0	100.00%	90	95.65%	230	89.53%		
F-Secure Internet Security	0	100.00%	0	100.00%	0	100.00%	30	98.55%	117	94.66%		
F-Secure Protection Services	0	100.00%	0	100.00%	0	100.00%	30	98.55%	117	94.66%		
G DATA AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.76%		
K7 Total Security	0	100.00%	5	99.61%	5	97.32%	883	68.95%	455	79.33%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	30	98.55%	72	96.73%		
Kingsoft Internet Security	0	100.00%	15	98.97%	87	81.89%	2009	42.15%	634	71.20%	1	
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	341	84.52%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	0	100.00%	90	95.65%	106	95.17%		
Norman Security Suite	0	100.00%	0	100.00%	7	99.15%	767	76.96%	128	94.18%		
NWI Virus Chaser	12	98.27%	0	100.00%	0	100.00%	90	95.65%	93	95.77%		2
PC Tools AntiVirus	0	100.00%	2	99.91%	8	99.21%	313	77.70%	381	82.69%		
PC Tools Spyware Doctor	0	100.00%	2	99.91%	8	99.21%	313	77.70%	404	81.64%		
Proland Protector Plus	6	99.99%	5	99.48%	56	92.76%	1722	46.38%	1969	10.48%		
Quick Heal AntiVirus	0	100.00%	53	93.15%	10	98.03%	908	81.51%	1465	33.40%		
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	90	95.65%	102	95.38%		
Rising Antivirus	0	100.00%	2	99.81%	41	94.33%	1302	52.19%	268	87.82%		
Sophos Endpoint Security & Control	0	100.00%	0	100.00%	0	100.00%	90	95.65%	46	97.93%		33
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	90	95.65%	38	98.29%		
Trustport Antivirus	0	100.00%	0	100.00%	0	100.00%	561	87.72%	40	98.20%		
VirusBuster Professional	0	100.00%	2	99.91%	8	99.21%	313	77.70%	362	83.56%		3
Webroot AntiVirus with AntiSpyware	0	100.00%	4	99.48%	0	100.00%	107	95.06%	48	97.81%		

CA AntiVirus + AntiSpyware 9.0.0.171

ItW	100.00%	**Polymorphic**	95.37%
ItW (o/a)	100.00%	**Trojans**	53.86%
Worms & bots	100.00%	**File infectors**	99.84%
False positives	1		

CA's home-user product is simple and speedy to set up, zipping through the standard options, EULAs and file copying in around a minute and a half; after this come options to install a *Yahoo!* toolbar and to set the browser to use *Yahoo!* for searching. Both of these options are checked by default and must be deselected if not required. After this, a reboot is needed.

Once again, to aid the less knowledgeable user and keep things simple, configuration is barely provided, but everything seemed to work pretty well. Scanning speeds were most impressive, and detection pretty solid, although a little weak in the new trojans set.

With the WildList covered without any problems, just a false positive in the clean set upset *CA*'s chances of an award for this product, and didn't bode well for the hopes of the company's corporate version.

CA eTrust 8.1.637.0

ItW	100.00%	**Polymorphic**	95.37%
ItW (o/a)	100.00%	**Trojans**	53.86%
Worms & bots	100.00%	**File infectors**	99.84%
False positives	1		

Setup of *eTrust* is a little more time-consuming, with EULAs in triplicate which must be scrolled through to the bitter end before they can be acknowledged, and a screen requesting a considerable amount of personal information to be filled in, again followed by a reboot.

The interface provided has always proved something of a bugbear during VB100 testing, but seemed a little faster and more responsive this time, perhaps thanks to the new, more powerful test hardware. There was still the occasional longueur as a screen prepared itself, and log viewing proved as awkward as ever. There was also an occasional problem with scans deactivating themselves while the interface presented a dialog box demanding credentials, although exactly what kind of credentials was not clear and simply cancelling out and reopening the interface got around this.

Once scanning was properly underway however, speeds were incredible as usual and detection rates again decent, with less thorough coverage of the trojans but no issues in the WildList. As expected, the same false positive put paid to *CA*'s chances of coming away with a VB100 award for either of the company's products.

eEye Digital Security Blink Professional 4.0.1

ItW	100.00%	**Polymorphic**	67.12%
ItW (o/a)	100.00%	**Trojans**	93.43%
Worms & bots	100.00%	**File infectors**	99.15%
False positives	0		

Initial installation of *eEye*'s *Blink* was simple and fast, but a few more steps had to be completed after the file copying, including licensing, a configuration wizard which could be cancelled to stick with the defaults, and offers to connect to the web to update and register the product. There followed a period of a minute or so while it settled in before the interface could be accessed.

The configuration is fairly in-depth, but lacks a 'block only' choice for the on-access scanner, meaning I had to let it destroy the test collection as it went through, but speeds were good enough for this not to matter much. Scanning of executables on demand was a little slower, thanks to the use of *Norman*'s sandbox technology to look for bad behaviours, but this attitude paid off with slightly better detection levels both for trojans and polymorphic viruses on demand, where the sandbox is used more deeply. There were no issues in the WildList in either mode, and no false positives either, meaning *eEye* can add another VB100 award to its growing collection.

ESET NOD32 Antivirus 3.0.667.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.84%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

ESET's installer, these days adorned with the rather groovy robot that has become the company's talisman, runs through a fairly standard set of options, with the whole thing running through from zero to protected in less than a minute and no reboot required.

With a splendid depth of options available in the advanced pages, more than plenty for the most demanding user, a few tweaks had everything just so and testing powered through in excellent time. A small issue appeared after scanning the full infected test sets in a single run on demand, in which the GUI appeared to hang and ceased to respond. Shutting it down with the task manager and restarting it soon put a stop to this however, and on-access scanning continued throughout this hiccup without issues. Detection rates were near perfect, and false positives absent, thus another VB100 award is added to *ESET*'s record tally.

Fortinet FortiClient 3.0.475

ItW	100.00%	**Polymorphic**	95.54%
ItW (o/a)	100.00%	**Trojans**	15.73%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The setup of *FortiClient* took a little longer, with a few more options needing to be set and a few lingering periods of waiting for activities to complete, but again no reboot was needed to activate the protection. The interface presented a familiar look, but seemed to be lacking the usual wealth of modules, perhaps indicating a pared-down version which would explain the less complex than usual setup process. Configuration is provided in great depth, but the defaults were pretty much just as I needed them and little

needed adjusting. Scanning speeds were very good, and detection rates generally superb, although performance in the trojans set was pretty disappointing. However, in the core WildList set there were no issues, and without false positives either *Fortinet* also notches up another VB100 award.

Frisk F-PROT Antivirus 6.0.9.1

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	89.53%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Frisk's desktop product provided one of the fastest setup processes of all, being completed in little more than 30 seconds, but did require a reboot, prior to which I judiciously dropped in the updates provided.

The product itself is one of the most basic, with barely any options available even for on-demand scans, which merrily deleted or cleaned files as it tripped through the test sets. This seemed to have little impact on scanning speeds however, which were pretty impressive, and detection rates were also solid, although one of the new batch of polymorphic viruses was not fully covered. With no false positives and no issues in the WildList, *Frisk* comfortably qualifies for a VB100 award.

F-Secure Internet Security 2009 9.00.146

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	94.66%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

F-Secure joins the growing group of vendors submitting multiple products, its *Internet Security Suite* being first up. The installation took a little time, including an automatic and unstoppable update attempt, and was followed by a reboot to complete the setup. Once up and running, the design was pretty familiar, little changed from the company's previous offerings, on the surface at least.

This meant a splendid array of tools and plenty of options available under the hood, providing excellent protection if not the best scanning speeds. Logging remains an issue, with records of completed scans rarely displayed in their entirety – HTML pages varied wildly in length but always missed off large amounts of detail, rendering data gathering somewhat difficult. Resorting to deleting files and seeing what was left behind showed the expected excellent coverage, with no problems in the WildList or clean sets and precious little missed elsewhere; a VB100 award is duly granted.

F-Secure Protection Services for Consumers

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	94.66%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

F-Secure's second offering is a customizable version of the company's suite designed for redistribution by ISPs wanting to provide branded protection to their customers. The setup and interface closely match the standard suite, with the basic components of anti-malware, web shield, spam filter and parental controls all available.

Speeds and detection rates also closely mirror the sister product, and the nasty logging was also in evidence. Quickly bypassing this showed the same results, granting *F-Secure* a second VB100 award this month.

G DATA AntiVirus 18.9.1.9

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.76%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The rather large installer file for *G DATA*'s product ran through its business pretty quickly and simply, requiring a system reboot to complete. Once up and running, a few changes were noted in the interface. These were most apparent in some changed wording in many of the options, and represented a number of small improvements to a thoroughly well-designed and usable tool.

G DATA also goes for a multi-engine approach, hence the large installer and slightly slower scanning speeds, but this is more than made up for by the superb thoroughness and excellent detection. Very little was missed, even in the new test set of trojans, particularly in the more thorough on-demand scans, and with no false positive issues and nothing missed in the WildList set, *G DATA* storms its way to another VB100 award.

On-demand throughput (MB/s)	Archive files - default		Archive files - all files		Binaries & system files - default		Binaries & system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - all files	
	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)
Agnitum Outpost	942	3.21	942	3.21	357	10.23	357	10.23	102	17.56	102	17.56	85	10.88	85	10.88
Ahnlab V3	476	6.35	476	6.35	682	5.36	682	5.36	94	19.06	94	19.06	59	15.68	59	15.68
Alwil avast!	32	94.52	628	4.82	218	16.76	259	14.11	36	49.77	79	22.68	28	33.04	56	16.52
ArcaBit ArcaVir	351	8.62	351	8.62	315	11.60	315	11.60	38	47.15	38	47.15	66	14.02	66	14.02
AVG Internet Security	1497	2.02	1784	1.70	375	9.74	380	9.61	478	3.75	486	3.69	42	22.03	143	6.47
Avira AntiVir	329	9.19	367	8.24	112	32.62	114	32.05	41	43.70	51	35.13	33	28.04	45	20.56
BitDefender AntiVirus	335	9.03	1203	2.51	520	7.03	556	6.57	67	26.74	73	24.54	85	10.88	89	10.40
Bullguard	1193	2.54	1193	2.54	578	6.32	578	6.32	74	24.21	74	24.21	93	9.95	93	9.95
CA AntiVirus + AntiSpyware	404	7.49	404	7.49	94	38.87	94	38.87	42	42.66	42	42.66	35	26.43	35	26.43
CA eTrust	207	14.61	207	14.61	82	44.56	82	44.56	23	77.90	23	77.90	28	33.04	28	33.04
eEye Blink Professional	511	5.92	511	5.92	1749	2.09	1749	2.09	55	32.58	55	32.58	149	6.21	149	6.21
ESET NOD32 Antivirus	841	3.60	841	3.60	553	6.61	553	6.61	39	45.94	39	45.94	48	19.27	48	19.27
Fortinet FortiClient	271	11.16	271	11.16	499	7.32	499	7.32	36	49.77	36	49.77	51	18.14	51	18.14
Frisk F-PROT Antivirus	259	11.68	259	11.68	432	8.46	432	8.46	39	45.94	39	45.94	36	25.70	36	25.70
F-Secure Internet Security	1303	2.32	1620	1.87	306	11.94	313	11.67	43	41.67	99	18.10	30	30.84	91	10.17
F-Secure Protection Services	1322	2.29	1681	1.80	310	11.79	313	11.67	43	41.67	97	18.47	30	30.84	108	8.57
G DATA AntiVirus	1415	2.14	1415	2.14	424	8.62	424	8.62	122	14.69	122	14.69	90	10.28	90	10.28
K7 Total Security	196	15.43	N/A	N/A	247	14.79	247	14.79	35	51.19	35	51.19	38	24.35	38	24.35
Kaspersky Anti-Virus	582	5.20	582	5.20	164	22.28	164	22.28	47	38.12	47	38.12	34	27.21	34	27.21
Kingsoft Internet Security	168	18.00	N/A	N/A	1541	2.37	1541	2.37	548	3.27	548	3.27	1019	0.91	1019	0.91
McAfee VirusScan	50	60.49	778	3.89	753	4.85	746	4.90	76	23.57	73	24.54	101	9.16	99	9.35
MWTI eScan Internet Security	1376	2.20	1376	2.20	885	4.13	885	4.13	858	2.09	858	2.09	883	1.05	883	1.05
Norman Security Suite	532	5.69	532	5.69	1753	2.08	1753	2.08	56	31.99	56	31.99	139	6.66	139	6.66
NWI Virus Chaser	1332	2.27	1332	2.27	665	5.49	665	5.49	132	13.57	132	13.57	136	6.80	136	6.80
PC Tools AntiVirus	458	6.60	N/A	N/A	276	13.24	276	13.24	67	26.74	67	26.74	73	12.67	73	12.67
PC Tools Spyware Doctor	976	3.10	976	3.10	611	5.98	611	5.98	82	21.85	82	21.85	91	10.17	91	10.17
Proland Protector Plus	250	12.10	N/A	N/A	133	27.47	133	27.47	63	28.44	63	28.44	88	10.51	88	10.51
Quick Heal AntiVirus	153	19.77	342	8.84	65	56.21	65	56.21	50	35.83	53	33.80	37	25.01	45	20.56
Redstone Redprotect	1221	2.48	1221	2.48	427	8.56	427	8.56	302	5.93	302	5.93	313	2.96	313	2.96
Rising Antivirus	926	3.27	926	3.27	555	6.58	555	6.58	80	22.40	80	22.40	91	10.17	91	10.17
Sophos Endpoint Security & Control	47	64.35	831	3.64	305	11.98	323	11.31	47	38.12	68	26.35	35	26.43	87	10.63
Symantec Endpoint Protection	390	7.76	402	7.52	256	14.27	269	13.58	77	23.27	75	23.89	77	12.02	75	12.34
Trustport Antivirus	504	6.00	504	6.00	488	7.49	488	7.49	113	15.86	113	15.86	295	3.14	295	3.14
VirusBuster Professional	20	151.23	977	3.10	299	12.22	321	11.38	58	30.89	90	19.91	26	35.58	65	14.23
Webroot AntiVirus with AntiSpyware	834	3.63	834	3.63	1859	1.97	1859	1.97	91	19.69	91	19.69	63	14.69	63	14.69

K7 Total Security 9.5.0469

ItW	100.00%	**Polymorphic**	68.95%
ItW (o/a)	100.00%	**Trojans**	79.33%
Worms & bots	99.61%	**File infectors**	97.32%
False positives	0		

Unlike most AV installers, which simply warn users of potential problems if installing over existing protection software, *K7*'s installer includes a check for possible conflicting products, along with the usual steps. Nevertheless this is all done with remarkable speed. A reboot is required, which is followed by a friendly welcome splash screen.

The suite includes a firewall and anti-spam module as well as the anti-malware component. The interface is pleasantly laid out with a reasonable level of configuration available, and runs stably with impressive speeds. Detection rates were also impressive, with only some of the more obscure items in the polymorphic set causing any problems and the new trojan set was covered pretty well. The WildList was also well handled and without false positives *K7* nobly achieves a second VB100 award.

Kaspersky Anti-Virus 2009 8.0.0.337

ItW	100.00%	**Polymorphic**	98.55%
ItW (o/a)	100.00%	**Trojans**	96.73%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Kaspersky's latest version ups the ante a little, with a further sheen of glitz and slickness added to its already exemplary design and a selection of extra goodies dropped in. The installation is unexceptionable, taking a few minutes to run through a standard range of setup options and do the actual business, which is followed by a reboot.

With the expected excellent depth of configuration available this proved unproblematic, speeds were pretty good even using more thorough settings, and detection rates very strong. With the WildList covered effortlessly and the only alert raised on the clean sets being a warning that a few files in the archive were password protected and thus could not be guaranteed to be clean, *Kaspersky* ably earns another VB100 award.

Kingsoft Internet Security 2008.2.22.11

ItW	100.00%	**Polymorphic**	42.15%
ItW (o/a)	100.00%	**Trojans**	71.20%
Worms & bots	98.97%	**File infectors**	81.89%
False positives	1		

Kingsoft's products have had an uneven ride in recent months, with some successes and some problems. This occasion proved much the same. The installation process was pretty straightforward, and no reboot was required despite the product including a firewall. This was fortunate as several installations were needed.

The first few runs showed remarkably low detection rates, with large numbers of items missed despite having been picked up by the product on previous occasions. Although consistent in themselves, some kind of problem was suspected when compared with the product's earlier performances. A second attempt produced the same results, but on a third install, with the on-access test slowed down considerably, things picked up remarkably and the WildList was covered completely, with detection considerably less thorough elsewhere. The difficult question of whether this patchy performance merited a VB100 award was thankfully skirted, when a single file in one of the clean sets was mislabelled as malware, denying *Kingsoft* the award this time.

McAfee VirusScan Enterprise 8.5.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	84.52%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

McAfee's corporate product is one of few to have remained virtually unchanged in the two years since I took on the *VB* testing role, and I am thankful for it. The simple, unflashy setup is always clear, stable and thorough. The setup process proved as straightforward and worry-free as ever, and was completed in excellent time with no reboot required. The interface itself has a serious, business-like air about it, and provides all the fine-tuning options one would expect from an enterprise-class product.

Scanning speeds were very good and detection at its usual excellent level, with coverage of the new trojan set a little less complete than I might have expected but still more than decent. With no issues in the WildList or the clean sets, *McAfee* also takes away a VB100 award.

MWTI eScan Internet Security

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	95.17%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The anti-malware component of *MicroWorld*'s *eScan* is based on the *Kaspersky* engine, but with numerous additions of *MicroWorld*'s own the setup process takes its time running through multiple stages of configuration and installation. After several minutes it was all ready to go however, without the need for a reboot.

The interface has a blocky, somewhat retro look and proved a little slow to respond on occasion. Configuration seemed pretty thorough, but on one occasion the product reverted to deleting infected files despite being asked not to. This minor quibble aside, detection was as excellent as I expected, speeds a little on the slow side, but without false positives or WildList issues another VB100 award is easily earned.

Norman Security Suite 7.00

ItW	100.00%	**Polymorphic**	76.96%
ItW (o/a)	100.00%	**Trojans**	94.18%
Worms & bots	100.00%	**File infectors**	99.15%
False positives	0		

I had been looking forward to getting my hands on *Norman*'s new suite product, having had a few minor issues with the design of the company's previous product. Setup was pretty simple and speedy, including the offer of a 'Screensaver Scanner' which would run a scan automatically when the machine was not in use (more on which later). It also suggested that a reboot might be required, but this proved not to be the case.

My first look at the new interface was both pleasing and confusing. It took some time to show itself, but once up and running looked slick and cool and a little minimalist. In some cases this proved to be because elements took some time to render, or occasionally even failed to materialize at all. Configuration options were either less in-depth than I had hoped or simply so elusive that I didn't manage to find them. Occasionally buttons proved unresponsive and the whole interface froze or shut itself down from time to time.

The problems with the interface proved to have little effect on the level of protection provided, which proved stable and

File access lag time (s/MB)	Archive files - default		Archive files - all files		Binaries & system files - default		Binaries & system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - all files	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
Agnitum Outpost	60	0.02	N/A	N/A	470	0.13	N/A	N/A	190	0.10	N/A	N/A	178	0.17	N/A	N/A
Ahnlab V3	82	0.03	N/A	N/A	446	0.12	N/A	N/A	62	0.02	N/A	N/A	74	0.06	N/A	N/A
Alwil avast!	246	0.08	821	0.27	331	0.09	347	0.09	155	0.08	174	0.09	63	0.05	92	0.08
ArcaBit ArcaVir	78	0.03	N/A	N/A	327	0.09	N/A	N/A	32	0.01	N/A	N/A	24	0.01	N/A	N/A
AVG Internet Security	145	0.05	N/A	N/A	512	0.14	513	0.14	126	0.06	139	0.07	33	0.02	103	0.09
Avira AntiVir	34	0.01	305	0.10	127	0.03	124	0.03	48	0.02	61	0.02	30	0.01	57	0.04
BitDefender AntiVirus	312	0.10	861	0.28	527	0.14	559	0.15	85	0.04	94	0.04	105	0.10	109	0.10
Bullguard	350	0.12	350	0.12	580	0.16	N/A	N/A	36	0.01	N/A	N/A	19	0.00	N/A	N/A
CA AntiVirus + AntiSpyware	29	0.01	N/A	N/A	106	0.03	106	0.03	51	0.02	51	0.02	44	0.03	44	0.03
CA eTrust	24	0.01	N/A	N/A	96	0.02	96	0.02	50	0.02	50	0.02	43	0.03	43	0.03
eEye Blink Professional	60	0.02	N/A	N/A	295	0.08	295	0.08	68	0.03	68	0.03	117	0.11	117	0.11
ESET NOD32 Antivirus	11	0.00	N/A	N/A	65	0.01	65	0.01	48	0.02	48	0.02	43	0.03	43	0.03
Fortinet FortiClient	223	0.07	223	0.07	416	0.11	416	0.11	39	0.01	39	0.01	66	0.05	66	0.05
Frisk F-PROT Antivirus	71	0.02	N/A	N/A	465	0.12	465	0.12	48	0.02	48	0.02	42	0.03	42	0.03
F-Secure Internet Security	35	0.01	1461	0.48	276	0.07	465	0.12	63	0.03	177	0.09	41	0.03	150	0.14
F-Secure Protection Services	35	0.01	1474	0.49	266	0.07	771	0.21	61	0.02	181	0.09	39	0.02	153	0.15
G DATA AntiVirus	226	0.07	1256	0.41	408	0.11	510	0.14	135	0.07	227	0.12	124	0.12	153	0.15
K7 Total Security	52	0.02	N/A	N/A	250	0.07	350	0.09	49	0.02	49	0.02	50	0.04	50	0.04
Kaspersky Anti-Virus	23	0.01	76	0.02	152	0.04	154	0.04	75	0.03	87	0.04	52	0.04	69	0.06
Kingsoft Internet Security	82	0.03	N/A	N/A	1549	0.42	1549	0.42	553	0.30	553	0.30	1046	1.11	1046	1.11
McAfee VirusScan	40	0.01	254	0.08	367	0.10	355	0.09	67	0.03	63	0.03	84	0.07	84	0.07
MWTI eScan Internet Security	996	0.33	996	0.33	275	0.07	275	0.07	91	0.04	91	0.04	94	0.08	94	0.08
Norman Security Suite	47	0.01	N/A	N/A	313	0.08	313	0.08	70	0.03	70	0.03	112	0.10	112	0.10
NWI Virus Chaser	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
PC Tools AntiVirus	45	0.01	N/A	N/A	25	0.00	25	0.00	219	0.11	219	0.11	149	0.14	149	0.14
PC Tools Spyware Doctor	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Proland Protector Plus	18	0.01	N/A	N/A	126	0.03	N/A	N/A	38	0.01	N/A	N/A	21	0.00	N/A	N/A
Quick Heal AntiVirus	14	0.00	N/A	N/A	67	0.01	N/A	N/A	46	0.02	N/A	N/A	24	0.01	N/A	N/A
Redstone Redprotect	37	0.01	N/A	N/A	266	0.07	266	0.07	147	0.07	147	0.07	144	0.14	144	0.14
Rising Antivirus	66	0.02	511	0.17	278	0.07	578	0.15	93	0.04	91	0.04	105	0.10	101	0.09
Sophos Endpoint Security & Control	36	0.01	785	0.26	307	0.08	322	0.08	48	0.02	62	0.02	46	0.03	77	0.06
Symantec Endpoint Protection	27	0.01	N/A	N/A	199	0.05	199	0.05	55	0.02	55	0.02	49	0.03	49	0.03
Trustport Antivirus	501	0.17	501	0.17	512	0.14	512	0.14	125	0.06	125	0.06	186	0.18	186	0.18
VirusBuster Professional	33	0.01	N/A	N/A	279	0.07	286	0.07	42	0.01	65	0.03	28	0.01	59	0.05
Webroot AntiVirus with AntiSpyware	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

reliable. On-demand scanning was a little awkward, particularly in the speed tests as, looking away to another test system as it ran, I returned to find the screensaver had activated, thus stopping my requested scan and starting the default full system probe. With this deactivated, things moved on nicely, with good speeds and decent detection, including full WildList coverage and no false positive issues. *Norman*'s protection, if not its GUI, earns the company a VB100 award.

NWI Virus Chaser 5.0b

ItW	98.27%	**Polymorphic**	95.65%
ItW (o/a)	98.27%	**Trojans**	95.77%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

NWI has been absent from the test for some time, but a return to the test bench offered a chance to see how the company's product has progressed. An initial surprise was the use of an 'InstallShiend Wizard' (*sic*) to operate the installation, but this proved remarkably fast if not well proof-read, getting protection fully operational in under 20 seconds, with judicious clicking of 'next'.

The main interface remains much as I remembered it from earlier tests, its most notable quirk being a prominent set of options to configure the colour and decoration of the interface. Other configuration proved limited, and on-access scanning was not activated on simple file access, meaning the tests had to be carried out by copying files to the system. This skirted the on-access speed test, but on-demand speeds were decent and system slowdown was not noticeable. On occasion the interface froze or shut down, apparently due to unusually large logs, a situation unlikely to occur in the real world, but overall detection proved pretty impressive. A few items in the clean sets were alerted on as possible dangers in the wrong hands, but false positives were absent. The trojan set was not the product's strongest point, and in the WildList set a few of the most recent items were also missed, keeping the VB100 award just out of *NWI*'s grasp.

PC Tools AntiVirus 2008 5.0.0.14

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	82.69%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Archive scanning		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
Agnitum Outpost	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Ahnlab V3	OD	X	9	X	9	9	X	9	X	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast!	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
ArcaBit ArcaVir	OD	2	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	√	√
AVG Internet Security	OD	X	√	X	X	√	X	√	√	X
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
BitDefender AntiVirus	OD	X/√	X/√	√	X/√	X/√	X/8	1/√	X/8	√
	OA	X/√	X/√	√	X/√	X/√	X/8	1/√	X/8	√
Bullguard	OD	√	√	√	√	√	8	√	8	√
	OA	X	√	X	X	√	X	√	8	X
CA AntiVirus + AntiSpyware	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	X	√
CA eTrust	OD	X	√	√	√	√	√	√	X	√
	OA	X	X	1	X	X	X	1	X	√
eEye Blink Professional	OD	X	X	1	1	X	8	2	X	√
	OA	X	X	X	X	X	X	X	X	√
ESET NOD32 Antivirus	OD	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	4	√	√
	OA	X	√	√	√	√	√	4	√	√
Frisk F-PROT Antivirus	OD	1	√	√	√	√	√	√	√	√
	OA	1	X	2	X	X	X	2	2	√
F-Secure Internet Security	OD	X/√	5	5	5	5	2	5	5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
F-Secure Protection Services	OD	X/√	5	5	5	5	2	5	5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
G DATA AntiVirus	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	8/√	8/√	4/√	√
K7 Total Security	OD	X	1	1	1	1	X	1	X	√
	OA	X	X	X	X	X	X	X	X	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/4	X/4	X/4	X/4	X/5	X	X	X	√
Kingsoft Internet Security	OD	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
MWTI eScan Internet Security	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Security Suite	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
NWI Virus Chaser	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	4	√	9	X
PC Tools AntiVirus	OD	X	X	X	X	X	X	X	X	√
	OA	2	2	2	X	2	1	2	2	√
PC Tools Spyware Doctor	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Proland Protector Plus	OD	X	√	√	X	X	X	√	X	√
	OA	X	X	X/2	X	X	X	X/2	X	X/√
Quick Heal AntiVirus	OD	X/2	X/5	2/5	X	X/5	X/1	2/5	X	√
	OA	X	X	X	X	X	X	X	X	X
Redstone Redprotect	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Rising Antivirus	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X/√
Sophos Endpoint Security & Control	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	OD	X	3/√	3/√	3/√	3/√	1/5	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	√
Trustport Antivirus	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	√	X	√	√	√	√	√
VirusBuster Professional	OD	2	√	X/√	X	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot AntiVirus with AntiSpyware	OD	X	√	X	√	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	√

Key:

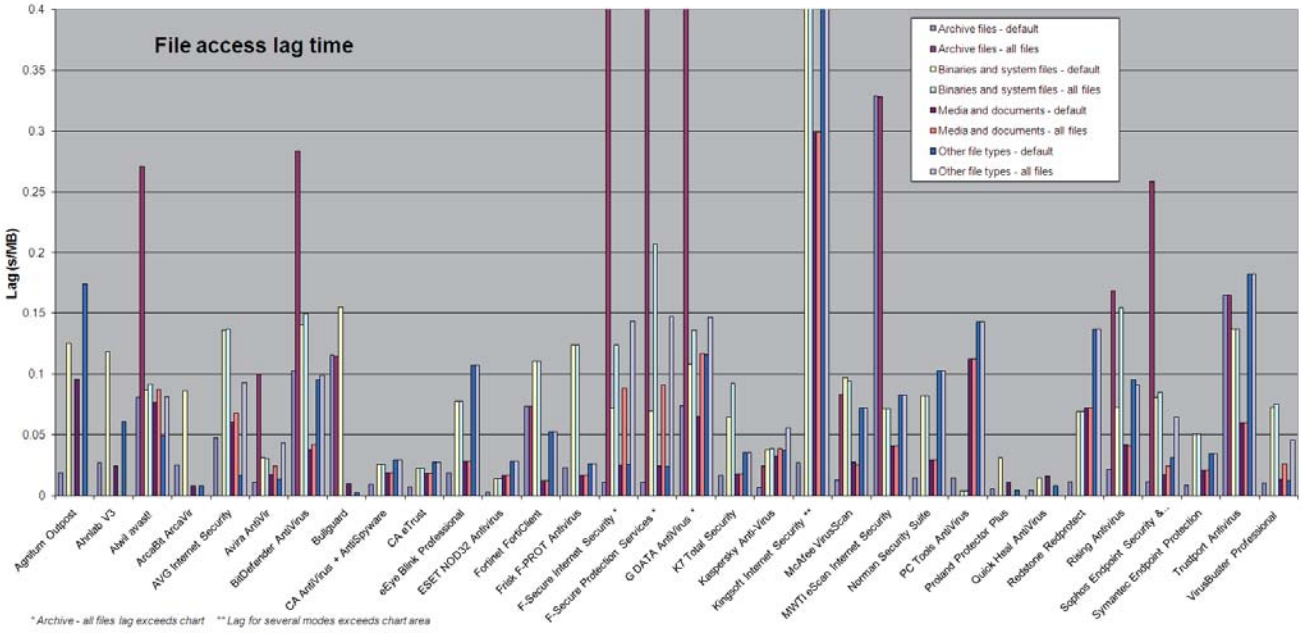
X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

[1-9] - Archives scanned to limited depth

X/√ - Default settings/thorough settings

*Executable file with randomly chosen extension



PC Tools products have produced many oddities in the past, and I approached them this month with my usual trepidation. The plain anti-virus product usually presents the fewest issues, and this time was no exception. Installing was fairly straightforward, with the product offering to install *Google* toolbars for me, and navigating the colourful, novice-friendly interface proved no problem. However, there were frequent lags moving from one page to another and configuration was minimal at best.

Scanning was completed fairly quickly, although the on-access behaviour seemed rather strange. Files were clearly being checked on simple opening, and scan times for most sets were rather slow, but executables seemed to be ignored entirely, hence the unusually fast time for this set.

Testing was thus performed by copying files to the systems and running scans with disinfection enabled, analysing remaining files for changes. As expected, final results showed fairly solid detection rates. False positives were absent, and the WildList covered in full, and thus *PC Tools AntiVirus* receives a VB100 award.

PC Tools Spyware Doctor 6.0.0.354f

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	81.64%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

Spyware Doctor is pretty similar to its sister product, but a little more tricky to configure and with even longer and more regular freezes, lags in accessing screens and other annoyances. Scanning behaviour seemed even more erratic, but generally items being copied to the system or scanned seemed eventually to be removed or disinfected, although this often took some time and seemed likely to leave the system at risk for a spell. With logging proving too vague and unreliable to give an accurate indication of what was happening, checking remaining files for changes was resorted to once again.

Once gathered, results proved to be along the same lines as for the plain anti-virus product, and thus *Spyware Doctor* also earns a VB100 award for its developers.

Proland Protector Plus 2008 8.0.C03

ItW	99.99%	**Polymorphic**	46.38%
ItW (o/a)	99.53%	**Trojans**	10.48%
Worms & bots	99.48%	**File infectors**	92.76%
False positives	0		

Proland is an occasional entrant in VB100 testing, known for its very compact, lightweight product. The 10 MB installer powered through its business in eyebrow-raising time, and no reboot was required to get things going.

A nice, clear, simple interface provided easy access to the required controls, although in-depth configuration was

minimal, and the speed tests zipped through at superb speed. False positives were absent, but detection was less than splendid, particularly in the trojan set and with polymorphic items in on-access mode. These polymorphic problems extended into the WildList set, where a few W32/Virut samples were missed in on-demand mode too, thus denying *Proland* a VB100 award for the time being.

Quick Heal AntiVirus Lite 9.50

ItW	100.00%	**Polymorphic**	81.51%
ItW (o/a)	100.00%	**Trojans**	33.40%
Worms & bots	93.15%	**File infectors**	98.03%
False positives	0		

Similarly small and lightweight, *Quick Heal*'s installation is also exceptionally speedy and completed in little over 30 seconds, without the need for a reboot.

The interface, glitzed up a little from previous versions, proved a little sluggish to respond on occasions, but scanning speeds and overheads were as excellent as ever. Detection across all test sets was reasonable, with false positives absent in the clean set after several such issues in recent tests. The WildList was handled without problems, and *Quick Heal* regains its VB100 certified status.

Redstone Redprotect 1.6.1.0

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	95.38%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Redstone's product implements the strong protection of the *Kaspersky* engine, with the .NET framework required for the front end. This added somewhat to the installation time, which was pretty fast once the framework was in place and requested no reboot. However, the product seemed not to have been started at the end of the process, so the system was restarted manually to ensure everything was in place.

Designed to be managed remotely, *Redprotect* has little by way of user configuration, simply a set of options accessible via the system tray icon to run manual scans and updates. A simple configuration tool is made available for testing purposes, basically adjusting registry entries which would otherwise be controlled by the remote manager. This proved just about enough for my needs, although the options to activate archive scanning in the on-access mode seemed not to function. Speeds in both modes were not super fast, and one of the on-demand scans of a subset of the clean collection repeatedly crashed out, but things were completed eventually and the somewhat awkward multiple logs gathered, linked up and parsed.

The results showed the excellent detection expected of the engine, an absence of false positives and flawless coverage of the WildList, earning *Redstone* a VB100 award.

Rising Antivirus 20.47.22

ItW	100.00%	**Polymorphic**	52.19%
ItW (o/a)	100.00%	**Trojans**	87.82%
Worms & bots	99.81%	**File infectors**	94.33%
False positives	0		

Rising's product had one of the most complex installation processes, running speedily but with a multitude of questions and options put before the user. Once done with, and after the required reboot, the interface is smooth and efficient-looking but on occasion slow to respond, as is the system as a whole, perhaps thanks to the cartoon lion placed on the desktop, constantly performing acrobatics, striking poses and so on, seemingly unrelated to the activities of the product.

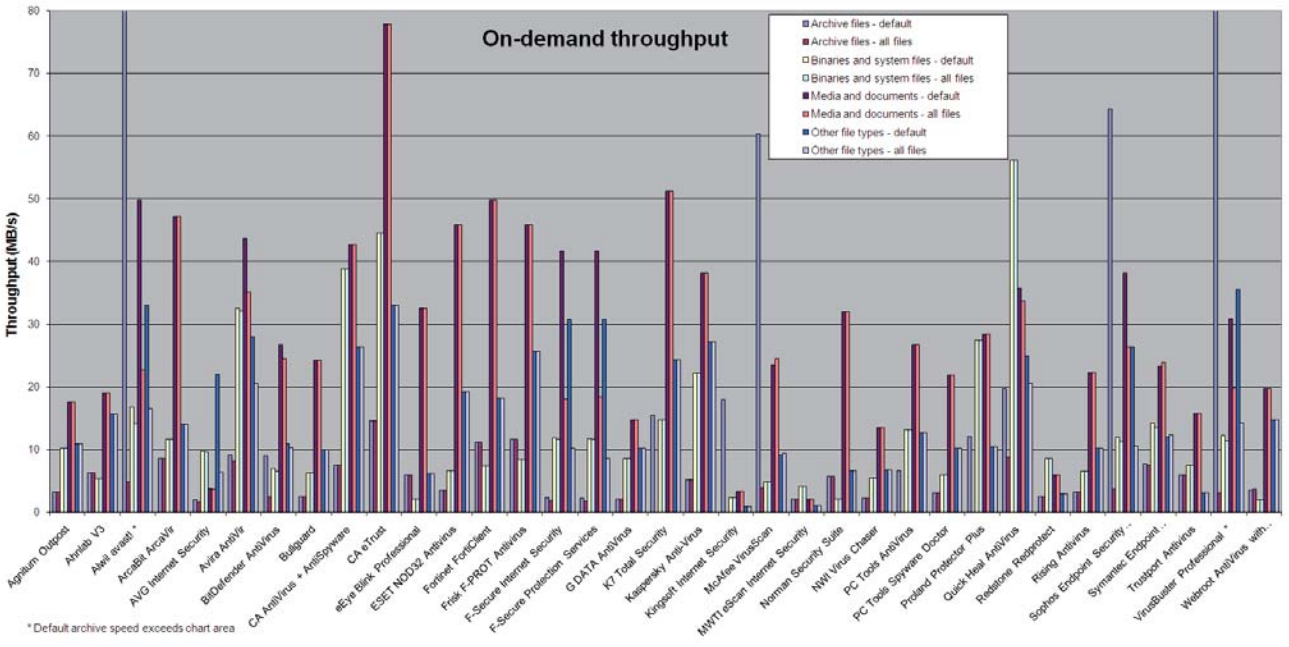
Despite this scanning speeds were reasonable, as was detection across the sets, and false positives were absent. Some initial worries that some samples of W32/Looked (aka Viking) were being missed on access proved to be a one-off, with everything on the WildList detected flawlessly on a second attempt, and *Rising* becomes the proud winner of its first VB100 award.

Sophos Endpoint Security & Control 8

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	97.93%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Sophos's latest product-naming scheme seems to reflect a marketing move rather than the product under test here, which remains much as normal. The installation is straightforward and includes the offer of a firewall, and also the removal of any 'third-party software'. It all ran through in under a minute and needed no reboot.

As an enterprise-focused product *Sophos* provides the most in-depth configuration anyone could ask for, all of which is



easily accessible. Speeds were good and detection excellent; a VB100 award is earned with ease.

Symantec Endpoint Protection 11.0.2000.1567

ItW	100.00%	**Polymorphic**	95.65%
ItW (o/a)	100.00%	**Trojans**	98.29%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

Like *Sophos*, *Symantec* also included the dreaded 'endpoint' euphemism in its product title, but its business-grade product is a little more bright, shiny and, well, less business-like. The installation took a few minutes, including the offer of some readmes and guides in PDF format. In the colourful interface, configuration is not hugely complex, much of this presumably being left to an admin with a management tool. One thing proved vital for my testing needs though: the option to up the priority of scanning, as an initial attempt at scanning the infected sets would have taken, by my estimation, around 13 days to complete (the fastest time for another product was seven minutes). This sluggishness can presumably be explained by various bits of logging and side-scanning being carried out when a detection is spotted, as scanning of the clean sets was pretty fast. Detection rates were splendid, false positives absent, and *Symantec* thus earns another VB100 award.

Trustport Antivirus 2.8.0.3003

ItW	100.00%	**Polymorphic**	87.72%
ItW (o/a)	100.00%	**Trojans**	98.20%
Worms & bots	100.00%	**File infectors**	100.00%
False positives	0		

The *Trustport* installer runs very quickly, the process completed in under a minute, with no unexpected options to break the chain of 'next's and no reboot required.

The layout of the product is a little odd, having no true main interface but instead several configuration pages and scanning tools accessible from the system tray icon. This system proved perfectly usable however, and provided ample controls for the product. The number of engines used by the product has varied considerably of late, but was down to a mere two this time, clearly a wise decision as scanning times were not as slow as they have been in the past while detection rates remained excellent. With not much missed and no false positives, *Trustport* also earns a VB100 award.

VirusBuster Professional 5.3.121

ItW	100.00%	**Polymorphic**	77.70%
ItW (o/a)	100.00%	**Trojans**	83.56%
Worms & bots	99.91%	**File infectors**	99.21%
False positives	0		

VirusBuster is a challenger for the fastest installation process, with its simple system which starts with a simple *WinZip* dialog and completes, after a standard set of choices, around 30 seconds later with no reboot required.

The interface is much as it has been for some time, a tried and trusted thing which, while occasionally a little awkward to navigate, provides plenty of configuration in stable and reliable style. The protection offered is similarly solid, with more than decent detection rates and very decent speeds. No issues in the WildList or clean sets means that *VirusBuster* earns a VB100 award.

Webroot AntiVirus with AntiSpyware 5.5.7.124

ItW	100.00%	**Polymorphic**	95.06%
ItW (o/a)	100.00%	**Trojans**	97.81%
Worms & bots	99.48%	**File infectors**	100.00%
False positives	0		

This product starts out as the traditional *SpySweeper* anti-spyware tool, before a few judicious additions – including the *Sophos* anti-virus engine – convert it, name and all, into a full anti-malware product. The install process is fairly straightforward and fast, complicated by the lack of web connection and need to manually doctor some sections, but things are soon up and running after a reboot.

The interface provides rather confusing access to a very limited configuration setup, and seemed even more sluggish in its response times than usual, especially when running on-demand scans. On-access detection is only sparked by copying files to the system, and seems to allow writing and then to remove the file when it gets round to it, in some cases quite some time later. Actually executing files seems to be blocked a little more promptly, but it still left me rather nervous.

This system meant on-access speeds could not be measured, but the machine seemed to be rather slow, and under heavy load the interface froze regularly – on occasion the whole system, but in most cases recovered without intervention, patience allowing. Logging was a little odd, in many cases failing to record any data on files removed or cleaned, so detection rates had to be measured by comparing checksums of remaining files. After this arduous process the expected solid detection was shown, including full WildList coverage and no false positives, and a VB100 award is duly granted.

CONCLUSIONS

This was another bumper test, with its usual crop of issues. Passes were plentiful, with a few false positive issues and a few products having problems with WildList samples. In particular the W32/Virut strains continue to fox products after several months on the WildList, during which time they have been consistent high-flyers in *VB*'s prevalence charts. The new trojan set proved informative, although as expected most AV labs managed to keep pretty much on top of *VB*'s sample-gathering and validation process. We anticipate removing most of the files used here from future test sets, using a rolling system to keep the set as up to date as possible, so hopefully some patterns of strength and weakness should begin to emerge over time.

The biggest issues this time around were with interface design and stability. A remarkable number of professionally made and presumably professionally tested products presented problems with their interfaces freezing, crashing, or being unbearably slow to respond, and in some cases this instability ran over to the protection offered and even brought down the entire test system. Whether any of these issues are influenced by the addition of the recent service pack remains to be investigated in post-test analysis. Software stability is pretty vital, particularly in security software, and a shaky interface will swiftly lose the trust of users even if the protection behind the scenes remains up and running. It never fails to astound me that products should reach external testers, and presumably also users, with such serious issues as have been seen in some this month.

This test marks something of the end of an era. For many years the VB100 has been a solo effort, carried out entirely by a single tester beavering away on his own in an empty test lab. In time for the next test (barring unforeseen problems), there will be two pairs of hands on the keyboards and two pairs of eyes on the screens. For me, this should mean the end of the long hours and late nights required, while for our readers it will mean more value and information from our tests, thanks to there being more time to devote to expansion, devising and implementing new tests and keeping sample sets broader and more up to date. For competing vendors, of course, this will mean stiffer challenges and tougher criticisms of failure, but then, not everyone can be a winner.

Technical details:

All products were tested on identical systems with *AMD Athlon64* X2 Dual Core 5200+ processors, 2 GB RAM, dual 80 GB and 400 GB hard drives, running *Microsoft Windows XP Professional* (32-bit) with Service Pack 3.