COMPARATIVE REVIEW

WINDOWS XP SP3

John Hawes

The VB100 returns to the evergreen *Windows XP* platform this month – all but guaranteed to provide the setting for the biggest and busiest comparative of the year.

Although expectations of a large field of competitors were not disappointed, our fears of numbers potentially pushing a close to unmanageable 50 products were not realized as submissions from a number of semi-regular entrants were not forthcoming. Despite these absences, an impressive range of 39 products from 34 different vendors made the cut for the 24 February deadline, with the regular well-known brands accompanied by an interesting set of less well-known names and a handful of newcomers. Some of the newcomers hovered on the edge of meeting the requirements for qualification. In particular, the rules regarding a product's on-access functionality insist (for logistical purposes) on the ability to detect files on open or write rather than on full execution. It was decided that any product that could not be coaxed into responding to our test methodology would be excluded from the test.

With such a large and diverse field of products to test in a very limited time frame, the issue of multiple entries from single vendors posed some problems, and it became clear that it may be necessary in future to impose a small charge for vendors who wish to submit several versions of a product to the same test. This would enable us to invest in additional hardware – and potentially manpower – to cope with the testing of an ever-increasing number of products without compromising the essential free-to-all nature of the VB100 (entry of the first product would remain free of charge for every vendor). Details of any decisions we make in this direction will be made clear as part of the official VB100 procedures published on www.virusbtn.com.

This month also saw the first major set of results from our new RAP tests, which were introduced with a much smaller field of competition in the recent *Linux* test (see *VB*, February 2009, p.15). The data from this much larger set of products promised to provide some fascinating insights into many aspects of performance across the board.

PLATFORM AND TEST SETS

More than two years since the release of its successor, *Windows Vista*, more than seven years since its own first appearance, and just a few months since its official retirement from the market, *Windows XP* remains the dominant platform for computer users across the globe.

Anecdotal evidence from users in home, academic and corporate environments is backed up by usage statistics gathered from browser data on machines surfing the Internet, which show that *XP* continues to run on around 70% of desktop systems. *Vista*'s market penetration continues to increase slowly, with the platform now estimated to run on around 20% of systems. It remains to be seen if the advent of *Windows 7*, based on *Vista*'s innovations but with some considerable upgrades, will finally shake users' long-standing attachment to *XP* and herald a new era of computing.

The continued popularity of *XP* reflects its stability, simplicity and familiarity, and preparation of the test systems was a pretty straightforward task. Images used in the last test were adjusted slightly to cooperate with some minor changes in the test network, but were essentially left much as they stood. As per our standard procedures, no further updates beyond the Service Pack 3 level were added, which promised to give us some interesting results from the vulnerability detection features included in a selection of the latest generation of security suites. Otherwise, beyond tweaking the appearance and settings to fit our personal tastes, adding drivers to support the test hardware, and connecting to the lab servers to access sample and log storage, the test machines ran basic, bare and default *XP* setups.

The management of this month's test sets made for rather more work. The WildList deadline for the test was 20 February, a Friday fairly close to both the product deadline (24 February) and the usual release date of new WildLists. This caused some disquiet amongst developers anticipating a very short space of time in which to test their products against new samples added to the list. However, as it turned out, the January issue of the WildList emerged on 19 February, giving developers a little more time to make their checks.

The January WildList continued to be dominated by online gaming password stealers, and a large number of retirements from the list meant that the bulk of the items commonly seen of late, including W32/Mytob and the wide selection of network worms and bots, disappeared from the list.

Most notable among the new additions were a handful of samples representing the Conficker (aka Downadup) worm that is currently making waves around the world (see *VB*, March 2009, p.7). Breaking the monotony of simple static items was a single instance of W32/Fujacks (best known for the 'Panda burning Joss-sticks' icon that accompanied early versions). The inclusion of a file-infecting virus in the WildList set promised to provide a little extra challenge for labs, checking that they are still properly protecting against true viruses as well as the glut of more static malware.

The other test sets saw a little maintenance work as usual, with the polymorphic set having a few new items added to make up for some older items having been retired, while the trojan set was once again built from scratch using a few thousand new items gathered in the three months prior to testing. Work on the set of replicating worms and bots, which we had hoped to refresh completely in a similar manner to the trojan set, was put on the back-burner due to other priorities, but the set did undergo some expansion; we hope to find time to build a full replacement set for the next comparative.

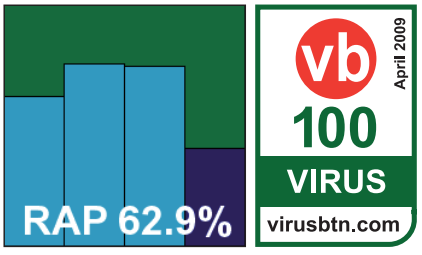
Most of the time set aside for the preparation of the test sets was devoted to building the sets for the RAP testing, with weekly sets built in the three weeks prior to the 24 February deadline and an additional set put together in the week after product updates were frozen ('week +1'). Once again we saw considerable fluctuation in the number of samples gathered in each week, but after classification and validation efforts we managed to build sets which we hoped would be suitably representative of the most prevalent malware as well as large enough to provide a good reflection of real-world performance against both known and unknown malware.

The clean test set also saw a fairly significant expansion, with updates to tracked software and a selection of new packages added. With the strict no-false-positives rule of the VB100 scheme, we endeavour to keep the clean test set as relevant as possible. However, it seems that fairly obscure false alerts – unlikely to impact many regular users – are increasingly becoming a major cause of products' failure to qualify for certification. We are investigating several options that would improve matters in this area, with one of the most important steps being the classification of clean samples according to prevalence and significance. It also seems that false positives are spreading more quickly between products these days, as automation plays a greater part in adding new detections and the samples shared between labs become polluted with clean samples. To circumvent the possibility of unscrupulous vendors exploiting this situation (by passing files known to be in our clean collection to their rivals in such a manner), we have removed from our sets several samples which have been alerted on in the past, thus ensuring that the contents of our sets remain unknown.

With everything prepared and in place a week after the product deadline, it was finally time to make a start on testing.

Agnitum Outpost Security Suite Pro 6.5.2514.381.0685

ItW	100.00%	**Polymorphic**	88.85%
ItW (o/a)	100.00%	**Trojans**	69.93%
Worms & bots	99.90%	**False positives**	0



Agnitum's *Outpost* suite has performed pretty well in our tests over the past few years, and has proved popular with the test team with its simple and clear design and stable performance. Installation took rather a long time, a particularly slow part of the process being the installation of *Microsoft* C++ libraries, but the product is a fairly complete suite including a very highly regarded firewall, so this is perhaps not too surprising. A reboot was required to complete the installation process.

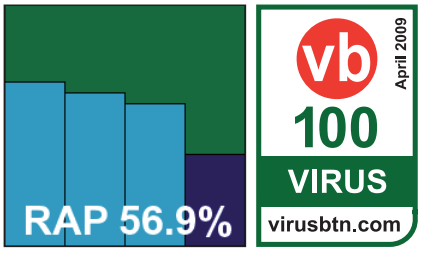
The product's interface remains unchanged, well laid out and easy to navigate. Configuration for the anti-malware component is pretty limited, but the defaults seem sensible and a decent level of protection is provided without adjustments, the on-demand scanner proving to scan much more deeply into archive types etc. than the on-access scanner. Running through the tests proved unproblematic, and results were fairly decent. Scanning speeds and overheads were mid-range, and detection rates were on the better side of average. A few polymorphic viruses were missed, and a steady if rather unimpressive catch rate was achieved across the trojan and RAP test sets, with an obvious drop in the 'week +1' set as expected. It should be noted that the product includes a plethora of additional protection measures that were not tested under our procedures – notably, the combination of firewall and HIPS protection, which would provide a better level of security than simple static detection.

The WildList presented no problems for the product, and without any false positives in the clean set *Agnitum* achieves the first VB100 award of this month's comparative.

AhnLab V3 Internet Security 7 Platinum 7.6.4.1 b.849

ItW	100.00%	**Polymorphic**	99.63%
ItW (o/a)	100.00%	**Trojans**	71.43%
Worms & bots	99.85%	**False positives**	0

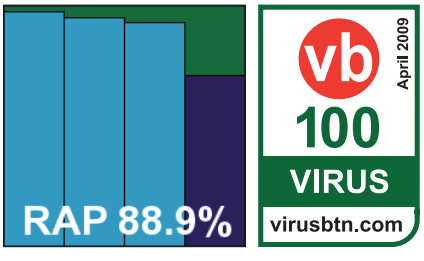
AhnLab's product offers a similar range of functionality but installed much more quickly, with fewer options to deal with and no reboot required. The interface is again clean and simple, with the emphasis firmly on the standard anti-malware side of things and the additional functions positioned less prominently. The layout was generally fairly sensible, with a few options tucked away in unexpected places, and again configuration was somewhat minimal.



Scanning speeds were not the quickest, but on-access overheads were fairly low. Detection rates were pretty average, not hugely impressive in the trojan or RAP sets and with a rather marked decrease in the unseen 'week +1' samples. However, the product has firewall and intrusion-prevention technologies (untested here) which would supplement the protection offered in a real-world situation. There were no false positives, although all *Microsoft Office* documents with macros attached were alerted on, with the product offering the option to remove the macros. The WildList was also covered without difficulty, and a VB100 is thus awarded.

Alwil avast! 4.8 Professional 4.8.1338

ItW	100.00%	**Polymorphic**	99.40%
ItW (o/a)	100.00%	**Trojans**	97.22%
Worms & bots	99.90%	**False positives**	0



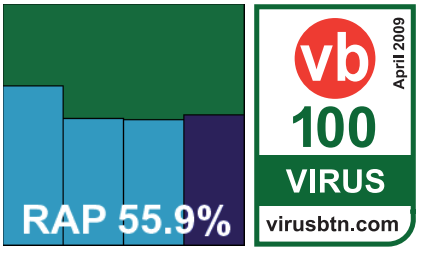
Alwil's product has been achieving some scorching detection rates in recent tests – both our own and those of other independent testing organizations – and we looked forward to seeing if these high standards could be maintained. The product's design has changed little over several years of tests, and the installation process is fairly quick and easy, but does require a reboot to complete. Although the layout has always seemed a little awkward and ungainly, the advanced version of the interface provides ample configuration options and testing ran through smoothly without incident.

Detection rates did indeed prove to be exceptional, with high levels across all our standard sets and over 90% in the first three weeks of the RAP sets. The drop in the 'week +1' test set was noticeable, but a respectable tally was achieved, and the pattern across the four weeks' worth of RAP sets was exactly what we would expect: a gradual decrease over the first three sets followed by a sharper decline as products venture into unknown territory. Scanning speeds were lightning fast, although on-access overheads were in the middle of the field. The product had no problems meeting the requirements for VB100 certification, which is duly awarded.

On-demand detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean Sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.90%	191	88.85%	1925	69.93%	0	0
AhnLab V3	0	100.00%	3	99.85%	24	99.63%	1829	71.43%	0	0
Alwil avast!	0	100.00%	2	99.90%	7	99.40%	178	97.22%	0	0
Authentium Command	0	100.00%	0	100.00%	167	98.75%	1962	69.35%	0	1
AVG	0	100.00%	1	99.95%	22	99.31%	272	95.75%	0	0
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	59	99.08%	0	0
BitDefender	0	100.00%	0	100.00%	0	100.00%	383	94.02%	0	0
BullGuard	0	100.00%	0	100.00%	0	100.00%	298	95.34%	0	0
CA AV	0	100.00%	0	100.00%	860	93.83%	3206	49.91%	0	0
CA eTrust	0	100.00%	0	100.00%	860	93.83%	3216	49.76%	0	0
Check Point Zone Alarm	0	100.00%	0	100.00%	0	100.00%	444	93.06%	0	0
eEye Blink	11	99.55%	0	100.00%	205	84.22%	1198	81.28%	0	0
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	302	95.28%	0	0
Filseclab Twister	53	86.85%	342	83.44%	4131	30.25%	2127	66.77%	21	4
Finport Simple	266	36.72%	732	64.55%	5099	16.47%	4814	24.79%	12	0
Fortinet FortiClient	0	100.00%	0	100.00%	4	99.66%	5989	6.44%	0	0
Frisk F-PROT	0	100.00%	0	100.00%	164	98.90%	1967	69.27%	0	0
F-Secure	0	100.00%	0	100.00%	0	100.00%	435	93.20%	0	0
G DATA	0	100.00%	0	100.00%	0	100.00%	20	99.69%	0	0
K7 Total Security	0	100.00%	4	99.81%	1404	74.94%	558	91.28%	2	0
Kaspersky	0	100.00%	0	100.00%	0	100.00%	251	96.08%	0	0
Kingsoft (Standard)	0	100.00%	15	99.27%	2814	48.30%	5635	11.97%	0	0
Kingsoft (Advanced)	0	100.00%	24	98.84%	2579	52.00%	1661	74.05%	0	0
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	611	90.45%	0	0
Microsoft Forefront	0	100.00%	0	100.00%	575	95.09%	973	84.80%	0	0
Microsoft OneCare	0	100.00%	0	100.00%	575	95.09%	1066	83.35%	0	0
MWTI eScan	4	99.01%	0	100.00%	0	100.00%	313	95.11%	0	2
Norman Security Suite	10	99.79%	0	100.00%	273	83.21%	1207	81.14%	0	0
PC Tools AV	12	99.75%	4	99.81%	3838	18.55%	4972	22.32%	0	0
PC Tools IS	12	99.75%	3	99.85%	3838	18.55%	4942	22.79%	0	0
PC Tools SD	12	99.75%	3	99.85%	3838	18.55%	4942	22.79%	0	0
Quick Heal	0	100.00%	14	99.32%	201	95.09%	857	86.61%	0	0
Redstone RedProtect	0	100.00%	0	100.00%	0	100.00%	438	93.16%	0	0
Rising IS	1	99.75%	17	99.18%	1130	70.02%	2771	56.71%	10	0
Sophos Endpoint	0	100.00%	0	100.00%	762	89.25%	1057	83.49%	0	4
Symantec Endpoint	0	100.00%	0	100.00%	5	99.96%	545	91.49%	0	0
Trustport	10	99.79%	0	100.00%	27	98.56%	352	94.50%	0	0
VirusBuster	0	100.00%	3	99.92%	191	88.85	1939	69.71%	0	0
Webroot	0	100.00%	0	100.00%	775	89.16%	1120	82.50%	0	0

Authentium Command Anti-Malware 5.0.8

ItW	100.00%	**Polymorphic**	98.75%
ItW (o/a)	100.00%	**Trojans**	69.35%
Worms & bots	100.00%	**False positives**	0



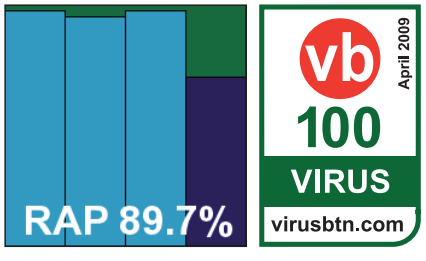
Authentium has been absent from our tests for some time now, and its product returns with a radical new interface designed using the .NET framework. Installation was a straightforward and rapid process, with a custom update system provided for our lab's unusual situation. The interface proved very simple and clearly laid out, with barely any options or configuration to trouble the user – it seemed impossible even to persuade the on-access scanner to check files with non-standard extensions. Reporting also proved rather unmanageable, but results were eventually gathered successfully after a few wrong turns signalled by figures that were way off the expected mark.

When full results were obtained, detection rates still proved rather lower than anticipated in the RAP sets. However, the product fared rather better in the standard sets – including the trojan collection, whose contents are not much older than the samples in the RAP sets and come from much the same sources. Scanning speeds were less than brilliant, but overheads were very reasonable. Nothing was missed in the WildList set, and a single item in the clean set that was alerted on with a vague level of suspicion was adjudged insufficient to prevent *Command* from winning a VB100 award.

AVG 8.0 b 237

ItW	100.00%	**Polymorphic**	99.31%
ItW (o/a)	100.00%	**Trojans**	95.75%
Worms & bots	99.95%	**False positives**	0

AVG's latest iteration includes yet more of the additional functionalities the company seems to be buying in at great speed of late. The design is as professional as ever, with a reasonably fast installation process followed by a 'first run wizard' to set some basic configuration options, followed by a reboot. The interface features an over-abundance of status icons, some of them apparently overlapping or of rather exaggerated significance, but tunnelling down to the advanced options proved no problem and everything we needed was readily to hand.

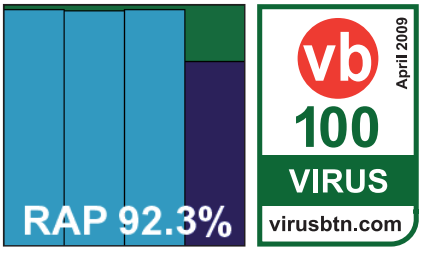


Both scanning speeds and overheads were around the middle of the pack, but detection rates were excellent, missing an overall average of 90% in the RAP sets by just a whisker. The product is another full security suite that provides a range of additional features, including the famous *LinkScanner* as well as the more standard likes of firewall, intrusion prevention, mail and web filters and much else besides, so real-world protection levels are likely to be even higher.

The product encountered no problems in detecting all samples in the WildList set, and generated no false positives in the clean sets, and as a result *AVG* achieves another VB100 award.

Avira AntiVir Professional 8.2.0.612

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.08%
Worms & bots	100.00%	**False positives**	0



Avira's product is another which has put in some truly remarkable performances over the last few years, and it continues to excel in a number of independent measures. With the bar for the new RAP tests already set pretty high, we looked forward to another likely candidate to push the bar and set the pace.

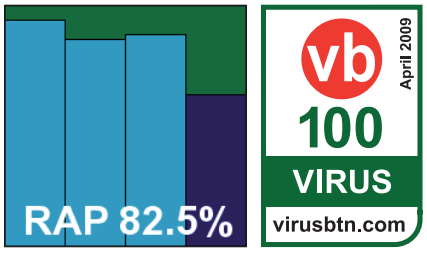
The product has changed little outwardly over the past few years, remaining adorned with friendly faces carrying red umbrellas, and featuring the occasional oddity of layout or syntax but generally proving simply laid out and responsive.

Running through the tests proved a simple process given the ample configuration options and very sensible defaults, and both scanning speeds and on-access overheads were excellent. Detection rates, as hoped, were similarly superlative, with very little missed anywhere. A more than decent score in the RAP 'week +1' set pushed the product's average RAP score to over 90% – the first product to achieve this milestone this month and likely to be one of very few to do so. With nothing to trouble the product in the

clean or WildList sets, a VB100 award is earned along with considerable respect.

BitDefender Total Security 2009 12.0.11.5

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.02%
Worms & bots	100.00%	**False positives**	0



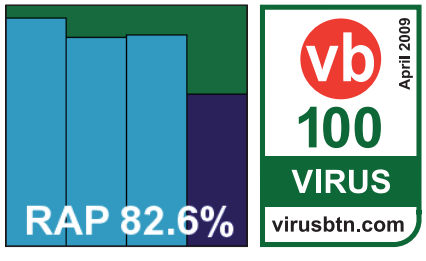
BitDefender returns after a brief absence from VB100 tests, with yet another revamping of the product's interface to reflect some significant changes under the hood. The installation process took a little time, but the new interface looked pretty good, with a nice simple version displaying status information accompanied by an advanced option with more detailed controls.

Scanning speeds were a little below expectation, but on-access overheads were very reasonable, and detection rates decent. Excellent scores were achieved in the standard sets and most of the RAP sets, and only an average-sized decrease in the 'week +1' set brought the product's RAP score down. Yet again, a wide range of additional protection levels are offered by the product, notable amongst which are a vulnerability monitor to check for out-of-date software and the data leak prevention options. The product encountered no problems in the WildList set, and with no problems in the clean sets either a VB100 is well earned.

BullGuard 8.5

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.34%
Worms & bots	100.00%	**False positives**	0

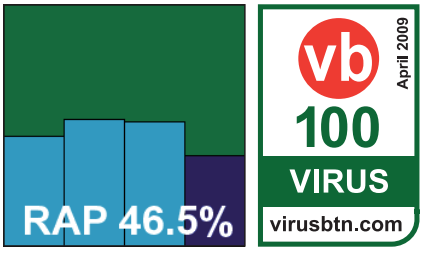
BullGuard's product seems to be making increasing inroads into various markets, thanks not least to free trials coming pre-installed on an impressive range of new hardware. Using the *BitDefender* engine, we expected similar scores and performance. Installation of the product was certainly similarly languorous, and included the rare offer to remove any potentially clashing competitive software. A reboot was required to complete the process. Initially, the product appeared to be misbehaving somewhat, and while a second reboot fixed some on-access issues, the interface frequently proved unresponsive, taking long pauses before responding even under normal activity levels. Logging and selection of post-scan options also proved a little awkward.



Detection rates, however, were excellent – actually showing a fractional improvement on those achieved by the *BitDefender* product, implying that *BullGuard* has either added some extra heuristics of its own or is using slightly stricter settings by default. Once again, the WildList caused the product no problems, and the clean sets likewise, thus securing a VB100 award for *BullGuard*.

CA Anti-Virus 10.0.0.169

ItW	100.00%	**Polymorphic**	93.83%
ItW (o/a)	100.00%	**Trojans**	49.91%
Worms & bots	100.00%	**False positives**	0



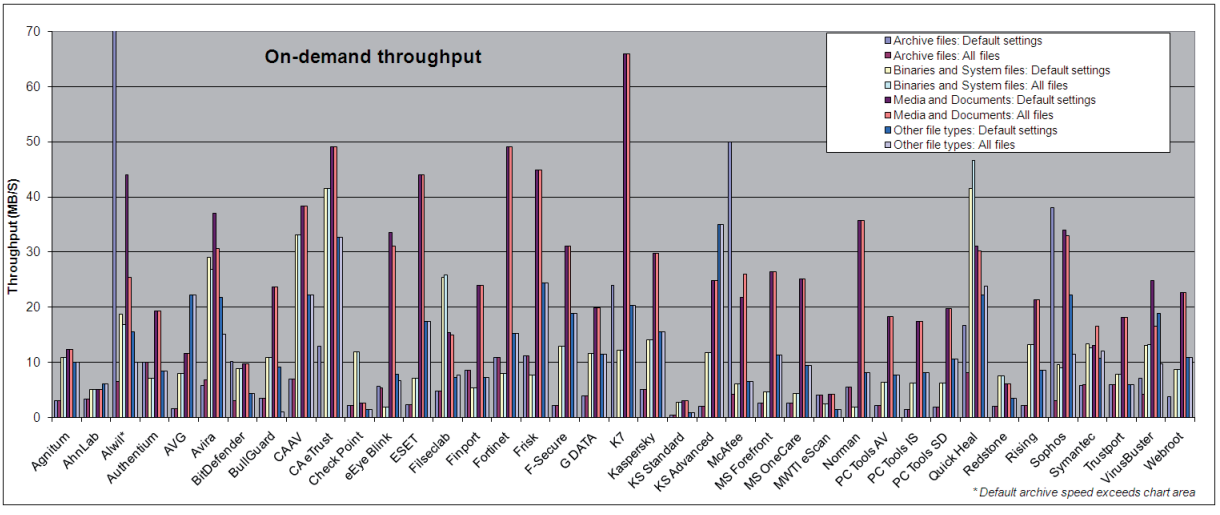
CA's home-user product has proved fairly reliable in recent tests, providing reasonable detection rates coupled with outstanding scanning speeds. Here the product remains little changed, although it surprised us somewhat during installation with an unavoidable attempt to update and with the proposal to install a *Yahoo! Toolbar*. A reboot was required to get things up and running. The interface itself remains clear and simple, with a fairly standard layout making for good usability. As expected, configuration was limited to little more than on or off, but scanning speeds and overheads were every bit as excellent as hoped.

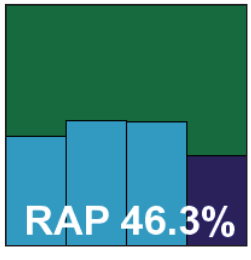
Detection rates lagged a little behind the curve, with stable but disappointing detection rates across the trojans and RAP sets. Elsewhere things were a little better, and with no issues in the WildList or clean sets a VB100 certification is awarded.

CA eTrust Anti-Virus 8.1.637.0

ItW	100.00%	**Polymorphic**	93.83%
ItW (o/a)	100.00%	**Trojans**	49.76%
Worms & bots	100.00%	**False positives**	0

On-access detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.90%	191	88.85%	1967	69.27%	0	0
AhnLab V3	0	100.00%	11	99.47%	24	99.63%	1833	71.36%	0	0
Alwil avast!	0	100.00%	2	99.90%	7	99.40%	173	97.30%	0	0
Authentium Command	0	100.00%	0	100.00%	167	98.75%	1977	69.11%	0	1
AVG	0	100.00%	1	99.95%	22	99.31%	272	95.75%	0	0
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	61	99.05%	0	0
BitDefender	0	100.00%	0	100.00%	0	100.00%	332	94.81%	0	0
BullGuard	0	100.00%	11	99.47%	0	100.00%	299	95.33%	0	0
CA AV	0	100.00%	0	100.00%	860	93.83%	3214	49.79%	0	0
CA eTrust	0	100.00%	0	100.00%	860	93.83%	3216	49.76%	0	0
Check Point Zone Alarm	0	100.00%	0	100.00%	0	100.00%	619	90.33%	0	0
eEye Blink	11	99.55%	0	100.00%	555	79.88%	1311	79.52%	0	0
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	251	96.08%	0	0
Filseclab Twister	53	86.85%	373	81.94%	4131	30.25%	2221	65.30%	8	0
Finport Simple	266	36.72%	756	63.39%	5099	16.47%	4814	24.79%	12	0
Fortinet FortiClient	0	100.00%	0	100.00%	4	99.66%	5984	6.51%	0	0
Frisk F-PROT	0	100.00%	0	100.00%	164	98.90%	1976	69.13%	0	0
F-Secure	0	100.00%	0	100.00%	0	100.00%	589	90.80%	0	0
G DATA	0	100.00%	0	100.00%	0	100.00%	31	99.52%	0	0
K7 Total Security	0	100.00%	4	99.81%	1593	71.33%	595	90.70%	2	0
Kaspersky	0	100.00%	0	100.00%	0	100.00%	628	90.19%	0	0
Kingsoft (Standard)	0	100.00%	17	99.18%	2814	48.30%	5665	11.50%	0	0
Kingsoft (Advanced)	0	100.00%	27	98.69%	2579	52.00%	1740	72.82%	0	0
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	526	91.78%	0	0
Microsoft Forefront	0	100.00%	0	100.00%	575	95.09%	1118	82.53%	0	0
Microsoft OneCare	0	100.00%	0	100.00%	575	95.09%	1124	82.44%	0	0
MWTI eScan	4	99.01%	0	100.00%	0	100.00%	315	95.08%	0	0
Norman Security Suite	10	99.79%	0	100.00%	350	81.68%	1320	79.38%	0	0
PC Tools AV	12	99.75%	13	99.37%	3838	18.55%	5266	17.73%	0	0
PC Tools IS	12	99.75%	11	99.47%	3838	18.55%	5103	20.28%	0	0
PC Tools SD	12	99.75%	11	99.47%	3838	18.55%	5103	20.28%	0	0
Quick Heal	0	100.00%	14	99.32%	201	95.09%	1835	71.33%	0	0
Redstone RedProtect	0	100.00%	0	100.00%	0	100.00%	633	90.11%	0	0
Rising IS	1	99.75%	14	99.32%	1212	66.36%	3006	53.04%	10	0
Sophos Endpoint	0	100.00%	0	100.00%	762	89.25%	1057	83.49%	0	3
Symantec Endpoint	0	100.00%	0	100.00%	5	99.96%	491	92.33%	0	0
Trustport	10	99.79%	0	100.00%	27	98.56%	352	94.50%	0	0
VirusBuster	0	100.00%	3	99.92%	191	88.85%	2012	68.57%	0	0
Webroot	0	100.00%	0	100.00%	775	89.16%	1146	82.10%	0	0



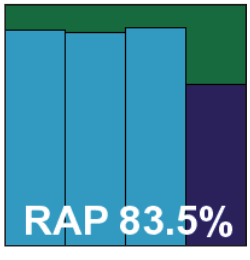


The corporate offering from *CA* has long been something of a bugbear in the VB100, its interface being approached with distaste and dread. The installation process, featuring numerous lengthy EULAs, is as tedious as ever, and the web-style interface (designed for corporate management no doubt) is awkward, fiddly, occasionally opaque, and often extremely slow to respond. Configuration is reasonably ample, although in some cases – such as adjusting archive scanning levels – proves not to react as expected.

Logging is also a little tricky to handle, with the on-screen displays not suited to handling more than a handful of issues at a time, but here experience helps, and our tried and tested techniques to extract data from their obscure format paid off. Once gathered, results showed the expected excellent scanning speeds in both modes. As in the home-user product, detection rates left much to be desired, but the product met all the requirements to achieve VB100 certified status. An award is granted, but a long overdue revamp of the front end remains high on our wish list.

Check Point Zone Alarm Extreme Security 8.0.298.000

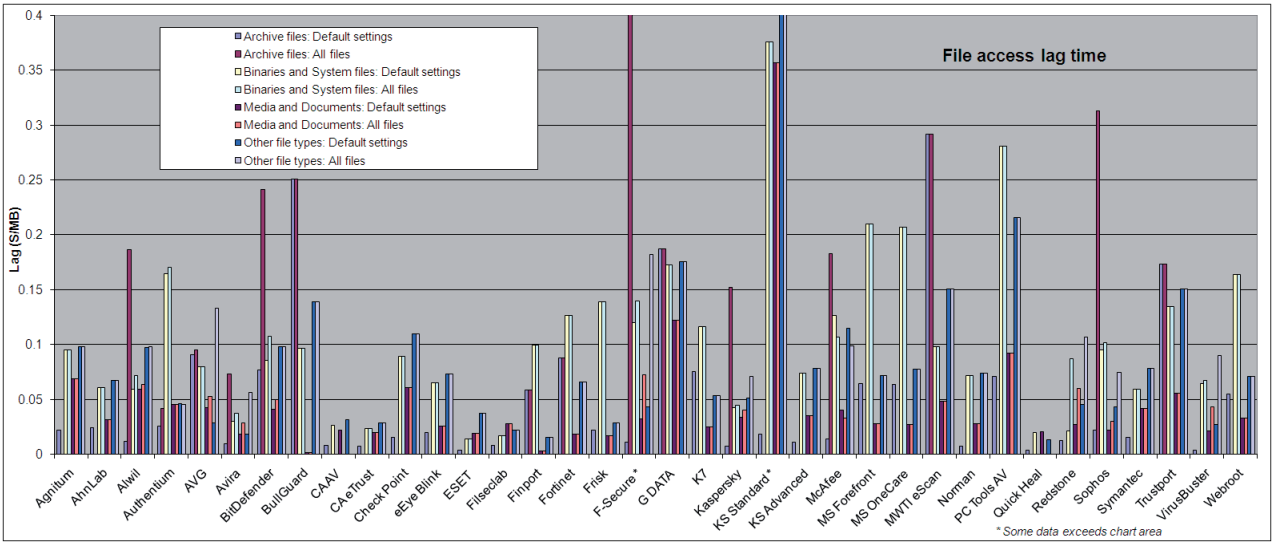
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.06%
Worms & bots	100.00%	**False positives**	0



Zone Alarm has only been entered for VB100 testing once before (see *VB*, April 2008, p.13). The initial installation process presented a few difficulties, with the basic package little more than a downloader for the installer proper. To accommodate the unusual submission style at short notice, the product was installed on a test system on the deadline date and updated online, with a dedicated image taken for later testing. However, it emerged that the 'update' button on the front page of the interface – which responded with a message claiming that the product was up to date – had not, in fact, functioned properly, as actioning a separate update within the anti-malware section of the product produced a much longer process and considerably higher version number. Updates were thus applied manually to one of the numerous folders sprinkled by the product around the system.

Scanning was also a little unconventional, with no clear option for manual scanning in the main interface; on-demand tests were thus performed using a combination of right-click scanning and scheduling. As the 'extreme' of the product title suggests, scanning was pretty thorough, which was reflected in rather slow on-demand scanning speeds, but on-access overheads were not unreasonable and detection rates were for the most part superb, thanks in part to the *Kaspersky* engine included in the product. The 'week +1' results in the RAP test showed a rather steeper downturn than average, from a very high starting point, but the product includes a wide range of extra protection features,

On-demand throughput (MB/s)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)
Agnitum Outpost	995	3.06	995	3.06	241	10.84	241	10.84	171	12.34	171	12.34	98	9.98	98	9.98
AhnLab V3	911	3.34	911	3.34	512	5.10	512	5.10	418	5.05	418	5.05	161	6.08	161	6.08
Alwil avast!	30	101.55	464	6.57	139	18.80	155	16.86	48	43.96	83	25.42	63	15.53	97	10.09
Authentium Command	303	10.05	303	10.05	369	7.08	369	7.08	109	19.36	109	19.36	116	8.43	116	8.43
AVG	1890	1.61	1890	1.61	326	8.02	326	8.02	182	11.59	182	11.59	44	22.23	44	22.23
Avira AntiVir	528	5.77	442	6.89	90	29.03	97	26.94	57	37.02	69	30.58	45	21.74	65	15.05
BitDefender	298	10.22	978	3.12	293	8.92	293	8.92	216	9.77	216	9.77	226	4.33	226	4.33
BullGuard	870	3.50	870	3.50	241	10.84	241	10.84	89	23.71	89	23.71	107	9.14	1007	0.97
CA AV	436	6.99	436	6.99	79	33.08	79	33.08	55	38.36	55	38.36	44	22.23	44	22.23
CA eTrust	235	12.96	NA	NA	63	41.48	63	41.48	43	49.07	43	49.07	30	32.61	30	32.61
Check Point Zone Alarm	1406	2.17	1406	2.17	220	11.88	220	11.88	820	2.57	820	2.57	680	1.44	680	1.44
eEye Blink	544	5.60	564	5.40	1387	1.88	1439	1.82	63	33.49	68	31.03	124	7.89	147	6.66
ESET NOD32	1306	2.33	1306	2.33	367	7.12	367	7.12	48	43.96	48	43.96	56	17.47	56	17.47
Filseclab Twister	633	4.81	643	4.74	103	25.37	101	25.87	137	15.40	141	14.96	134	7.30	127	7.70
Finport Simple	357	8.53	357	8.53	492	5.31	492	5.31	88	23.98	88	23.98	135	7.25	135	7.25
Fortinet FortiClient	278	10.96	278	10.96	325	8.04	325	8.04	43	49.07	43	49.07	64	15.29	64	15.29
Frisk F-PROT	273	11.16	273	11.16	337	7.75	337	7.75	47	44.89	47	44.89	40	24.46	40	24.46
F-Secure	1423	2.14	1423	2.14	202	12.94	202	12.94	68	31.03	68	31.03	52	18.81	52	18.81
G DATA	783	3.89	783	3.89	226	11.56	226	11.56	106	19.91	106	19.91	85	11.51	85	11.51
K7 Total Security	127	23.99	NA	NA	215	12.15	215	12.15	32	65.94	32	65.94	48	20.38	48	20.38
Kaspersky	595	5.12	595	5.12	186	14.05	186	14.05	71	29.72	71	29.72	63	15.53	63	15.53
Kingsoft (Standard)	7788	0.39	7788	0.39	970	2.69	970	2.69	707	2.98	707	2.98	1220	0.80	1220	0.80
Kingsoft (Advanced)	1505	2.02	1505	2.02	223	11.72	223	11.72	85	24.82	85	24.82	28	34.94	28	34.94
McAfee VirusScan	61	49.94	731	4.17	424	6.16	425	6.15	97	21.75	81	26.05	149	6.57	150	6.52
Microsoft Forefront	1153	2.64	1153	2.64	559	4.67	559	4.67	80	26.37	80	26.37	86	11.38	86	11.38
Microsoft OneCare	1146	2.66	1146	2.66	595	4.39	595	4.39	84	25.12	84	25.12	104	9.41	104	9.41
MWTI eScan	749	4.07	749	4.07	1052	2.48	1052	2.48	502	4.20	502	4.20	652	1.50	652	1.50
Norman Security Suite	558	5.46	558	5.46	1428	1.83	1428	1.83	59	35.76	59	35.76	121	8.09	121	8.09
PC Tools AV	1369	2.23	1369	2.23	410	6.37	410	6.37	115	18.35	115	18.35	128	7.64	128	7.64
PC Tools IS	2063	1.48	2063	1.48	423	6.18	423	6.18	121	17.44	121	17.44	120	8.15	120	8.15
PC Tools SD	1672	1.82	1672	1.82	417	6.27	417	6.27	107	19.72	107	19.72	92	10.63	92	10.63
Quick Heal	183	16.65	373	8.17	63	41.48	56	46.66	68	31.03	70	30.14	44	22.23	41	23.86
Redstone RedProtect	1536	1.98	1536	1.98	347	7.53	347	7.53	346	6.10	346	6.10	286	3.42	286	3.42
Rising IS	1410	2.16	1410	2.16	198	13.20	198	13.20	99	21.31	99	21.31	115	8.51	115	8.51
Sophos Endpoint	80	38.08	1010	3.02	274	9.54	291	8.98	62	34.03	64	32.97	44	22.23	85	11.51
Symantec Endpoint	520	5.86	507	6.01	196	13.33	207	12.62	162	13.02	128	16.48	91	10.75	81	12.08
Trustport	512	5.95	512	5.95	332	7.87	332	7.87	116	18.19	116	18.19	165	5.93	165	5.93
VirusBuster	431	7.07	733	4.16	201	13.00	197	13.26	85	24.82	128	16.48	52	18.81	101	9.69
Webroot	801	3.80	NA	NA	302	8.65	302	8.65	93	22.69	93	22.69	90	10.87	90	10.87

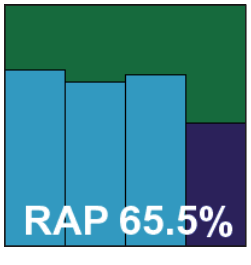


including advanced firewall and intrusion prevention technologies, which should go some way to improving matters in this area.

The WildList and clean sets presented no difficulties, and *Check Point*'s solid product earns its second VB100 award with its head held high.

eEye Digital Security Blink Professional 4.2.4.2076

ItW	99.55%	**Polymorphic**	84.22%
ItW (o/a)	99.55%	**Trojans**	81.28%
Worms & bots	100.00%	**False positives**	0

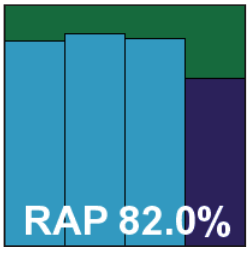


Blink is another semi-regular participant in our comparatives, with a good record in past tests and a reputation in our lab for combining impressive completeness of features with admirable clarity of design and usability. The installation process is lengthy but informative, and no reboot is required to complete, but many of the protection features appear to be disabled by default. This is not the case with the anti-malware portions, fortunately, which have a reasonable level of configuration in an interface which must ration space between numerous modules, notably vulnerability monitoring.

Scanning speeds were pretty good, with equally impressive on-access overheads, although scanning of large numbers of executables on demand did take some time thanks to the use of the *Norman Sandbox* technology. Detection rates were generally reasonable, with performance increasing notably with the age of samples. False positives were absent, but in the WildList set the selection of W32/Fujacks samples were missed, thus denying *eEye* aVB100 award this time.

ESET NOD32 3.0.684.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.28%
Worms & bots	100.00%	**False positives**	0



ESET's *NOD32* has long been a top performer in the VB100 and still holds the record for the largest number of certifications earned. The product has become considerably more stylish and user-friendly in recent years, but in some measures has lost its long-held lead in terms of both speed and detection rates, with some similarly excellent rivals catching up. The latest version is as slick and attractive as ever, and installation is a pleasant experience despite the occasional unexpected pause. Similar pauses were observed occasionally during scanning, particularly when handling large infected test sets, but such situations are vanishingly rare in the real world.

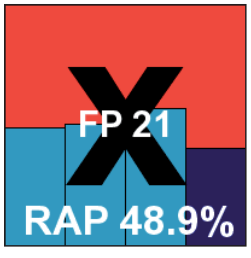
Scanning speeds and overheads over more normal types of data proved as excellent as ever – no longer way ahead of the field perhaps, but certainly among the very best. Detection rates were also excellent – again, not quite at the top of the heap, but putting in a very strong showing, with

File access lag time (s/MB)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (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	68	0.02	NA	NA	261	0.10	261	0.10	166	0.07	166	0.07	112	0.10	112	0.10
AhnLab V3	76	0.02	NA	NA	171	0.06	171	0.06	88	0.03	88	0.03	81	0.07	81	0.07
Alwil avast!	38	0.01	570	0.186	166	0.06	200	0.07	145	0.06	154	0.06	111	0.10	112	0.10
Authentium Command	81	0.03	130	0.042	442	0.16	458	0.17	117	0.05	116	0.05	61	0.05	60	0.05
AVG	277	0.09	292	0.095	219	0.08	219	0.08	110	0.04	132	0.05	44	0.03	146	0.13
Avira AntiVir	32	0.01	224	0.073	91	0.03	110	0.04	60	0.02	82	0.03	34	0.02	71	0.06
BitDefender	236	0.08	738	0.24	235	0.09	294	0.11	107	0.04	126	0.05	127	0.11	112	0.10
BullGuard	766	0.25	766	0.251	264	0.10	264	0.10	24	0.00	24	0.00	152	0.14	152	0.14
CA AV	27	0.01	NA	NA	81	0.03	NA	NA	67	0.02	NA	NA	46	0.03	NA	NA
CA eTrust	24	0.01	NA	NA	73	0.02	73	0.02	63	0.02	63	0.02	44	0.03	44	0.03
Check Point Zone Alarm	49	0.02	NA	NA	246	0.09	246	0.09	148	0.06	148	0.06	123	0.11	123	0.11
eEye Blink	62	0.02	NA	NA	183	0.07	183	0.07	74	0.03	74	0.03	87	0.07	87	0.07
ESET NOD32	12	0.00	NA	NA	48	0.01	48	0.01	60	0.02	60	0.02	52	0.04	52	0.04
Filseclab Twister	26	0.01	NA	NA	56	0.02	56	0.02	80	0.03	80	0.03	38	0.02	38	0.02
Finport Simple	181	0.06	181	0.059	271	0.10	271	0.10	28	0.00	28	0.00	31	0.02	31	0.02
Fortinet FortiClient	270	0.09	270	0.088	342	0.13	342	0.13	59	0.02	59	0.02	80	0.07	80	0.07
Frisk F-PROT	70	0.02	NA	NA	374	0.14	374	0.14	56	0.02	56	0.02	43	0.03	43	0.03
F-Secure	36	0.01	1555	0.510	325	0.12	377	0.14	89	0.03	173	0.07	58	0.04	194	0.18
G DATA	573	0.19	573	0.187	463	0.17	463	0.17	279	0.12	279	0.12	187	0.18	187	0.18
K7 Total Security	232	0.08	NA	NA	316	0.12	316	0.12	73	0.02	73	0.02	68	0.05	68	0.05
Kaspersky	25	0.01	466	0.152	122	0.04	129	0.04	91	0.03	106	0.04	66	0.05	85	0.07
Kingsoft (Standard)	58	0.02	NA	NA	995	0.38	995	0.38	773	0.36	773	0.36	1237	1.25	1237	1.25
Kingsoft (Advanced)	36	0.01	NA	NA	205	0.07	205	0.07	95	0.04	95	0.04	92	0.08	92	0.08
McAfee VirusScan	44	0.01	560	0.183	342	0.13	291	0.11	106	0.04	90	0.03	128	0.11	113	0.10
Microsoft Forefront	199	0.06	NA	NA	561	0.21	561	0.21	79	0.03	79	0.03	86	0.07	86	0.07
Microsoft OneCare	197	0.06	NA	NA	553	0.21	553	0.21	77	0.03	77	0.03	92	0.08	92	0.08
MWTI eScan	891	0.29	891	0.292	268	0.10	268	0.10	123	0.05	123	0.05	163	0.15	163	0.15
Norman Security Suite	25	0.01	NA	NA	198	0.07	198	0.07	79	0.03	79	0.03	88	0.07	88	0.07
PC Tools AV	218	0.07	NA	NA	745	0.28	745	0.28	215	0.09	215	0.09	227	0.22	227	0.22
Quick Heal	13	0.00	NA	NA	64	0.02	NA	NA	64	0.02	NA	NA	29	0.01	NA	NA
Redstone RedProtect	40	0.01	NA	NA	68	0.02	239	0.09	77	0.03	147	0.06	60	0.05	120	0.11
Sophos Endpoint	69	0.02	956	0.313	260	0.09	278	0.10	67	0.02	84	0.03	58	0.04	89	0.07
Symantec Endpoint	50	0.02	NA	NA	166	0.06	166	0.06	109	0.04	109	0.04	92	0.08	92	0.08
Trustport	529	0.17	529	0.173	363	0.13	363	0.13	138	0.06	137	0.06	163	0.15	163	0.15
VirusBuster	14	0.00	NA	NA	180	0.06	188	0.07	65	0.02	112	0.04	42	0.03	104	0.09
Webroot	169	0.05	NA	NA	441	0.16	441	0.16	90	0.03	90	0.03	85	0.07	85	0.07

a much lower drop in the 'week +1' RAP set than most. With the product encountering no problems meeting the requirements for VB100 certification, *ESET* adds another award to its sizeable collection.

Filseclab Twister AntiVirus 7.3.2.9971

ItW	86.85%	**Polymorphic**	30.25%
ItW (o/a)	86.85%	**Trojans**	66.77%
Worms & bots	83.44%	**False positives**	21



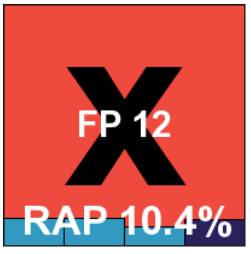
The first of the newcomers in this month's test, *Filseclab*'s *Twister* has picked up a bit of a reputation as a strong up-and-comer on various web forums and discussion boards, and has put in some excellent performances in independent tests run in China. An initial trial version we looked at impressed us with simplicity, stability and better than expected scanning performance, and a later version submitted for the test showed even more promise. With a slick and professional-looking installation process and a clear, attractive and well laid-out interface, the product certainly looks the business and has a very good level of fine-tuning available, as well as a behavioural monitoring system that is given as much importance as the more traditional detection in the layout of the interface.

Running through the tests proved a little less straightforward than hoped thanks to some slightly unusual behaviour: on-access scanning, while triggered on read, seemed not to block access instantly, instead waiting a little before alerting on and taking action against detected items. This meant that our standard opener tool, which logs items it cannot access, recorded having successfully opened everything. Thus, detection data could only be gathered from the product's own logs and the on-access scanning speeds, recorded in the same manner, may not quite reflect the full picture.

Detection rates were not unreasonable, particularly for a product that is entirely new to our testing system and test sets. Fairly good scores were achieved in some of the standard sets, including a surprisingly excellent handling of W32/Virut samples in the polymorphic set, with a little less coverage of older polymorphic items, and a fairly decent showing in the trojan and RAP sets. Several items in the WildList set were not covered, most of which were from the latest batch of additions, and a sprinkling of false alarms were raised in the clean sets (no big surprise on the product's first look at their diverse content), so *Twister* does not qualify for a VB100 award on its first attempt, but it looks like being a strong contender in the very near future.

Finport Simple Anti-virus 4.2.30

ItW	36.72%	**Polymorphic**	16.47%
ItW (o/a)	36.72%	**Trojans**	24.79%
Worms & bots	64.55%	**False positives**	12

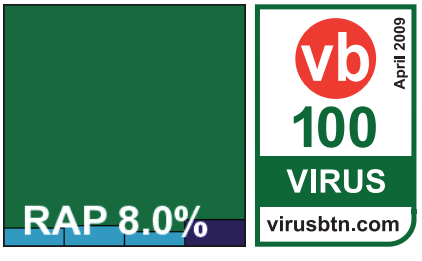


A second new product, this one emerging from the Ukraine and considerably newer on the scene, *Simple* lives up to its name in both its installation process and GUI, which uses the .NET framework and presents all the basic requirements in a very clear, easy-to-use manner. Bright, cheery, uncluttered and easy to navigate, the product stood up very well under the pressure of our tests, which can cause problems for much more seasoned solutions, running solidly and stably throughout.

Scanning speeds were pretty respectable, but detection rates still need a lot of work – which is not surprising for a product so very new to the scene. A smattering of false positives, along with quite a few misses in the WildList, deny *Finport* a VB100 this time, but the company's highly usable product will be very welcome in future tests, and we hope that with some work on detection levels it should soon reach the required standard for VB100 qualification.

Fortinet FortiClient 3.0.614

ItW	100.00%	**Polymorphic**	99.66%
ItW (o/a)	100.00%	**Trojans**	6.44%
Worms & bots	100.00%	**False positives**	0



Fortinet's desktop product has a much longer history in our tests, and has changed little since I first encountered it some years ago. The layout is serious and professional, with a number of additional protection features provided in a clean and uncluttered interface covering the wide range of configuration options required in corporate environments.

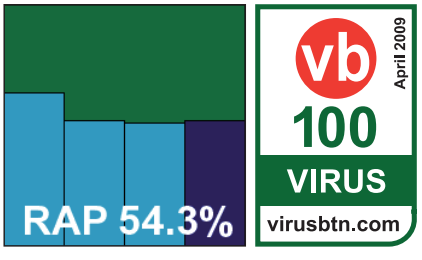
Scanning speeds and overheads were both excellent, and detection rates in our traditional test sets have long proved highly accomplished, but the addition of the new trojan sets in recent tests has highlighted some problems, and the low scores are repeated in the RAP sets here. The addition of optional 'grayware' scanning was tested – the absence of

which has been cited in previous tests as a possible reason for the low scores. The use of this scanning option did result in a small improvement over the rates recorded with the default settings, and enabling the 'heuristic' option (also disabled by default in the submitted product) increased detection rates substantially, to around 70% across the trojan and RAP sets. However, the vast majority of the additional detections were marked only as 'suspicious' – a tag which would not be counted as a full detection if this option were to be tested as part of the default settings.

Thankfully for *Fortinet*, no problems were encountered in the core certification test sets, with the product achieving full detection of samples in the WildList and generating no false positives in the clean sets. A VB100 award is duly granted.

Frisk F-PROT Anti-Virus 6.0.9.1

ItW	100.00%	**Polymorphic**	98.90%
ItW (o/a)	100.00%	**Trojans**	69.27%
Worms & bots	100.00%	**False positives**	0



Frisk's product remains a very simple and straightforward one, with few frills, minimal configuration and no extras beyond the basic requirements of anti-malware scanning and on-access protection.

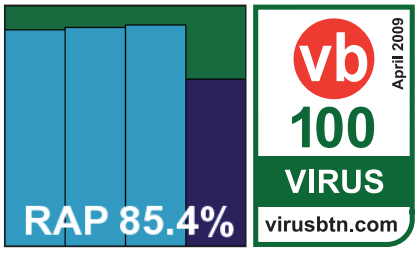
The installation process took a little longer than expected, with a long pause at the 'preparing to install' stage, and on several occasions during testing some stability issues were noted, both in general use of the interface and while running scans. On a few occasions the product generated error messages, but in most cases scanning or protection seemed to continue nevertheless.

Good scanning speeds were noted in the clean test sets, but results in the infected areas were harder to obtain thanks to freezes and other issues. Final figures were obtained after gently coaxing the product through the test sets, with a strong showing in the standard sets but rather lower figures seen in the new RAP sets – something of a disappointment after having achieved a remarkably high score in the first run of the RAP scheme in the recent *Linux* test. As on its previous outing, the product's detection system proved a little controversial, with an extremely finely graded range of detection flags including numerous combinations of vague and unusual terminology to report various levels of heuristic detections. However, even including the full range of 'security risk' and 'possible security risk' alerts – which we would usually adjudge to be only 'suspicious' detections and thus not counted as either detections in the standard sets or false positives in the clean sets – the detection numbers still lagged somewhat behind our high expectations.

Nevertheless, the WildList was covered without problems, and the clean sets likewise handled without issue, and a VB100 certification is awarded.

F-Secure Client Security 8.00 b.232

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.20%
Worms & bots	100.00%	**False positives**	0



F-Secure's desktop range continues to expand, but thankfully this busy month saw only the flagship product entered into the test.

The product continues to exert its icy charms with a speedy, informative setup process and an unusual but highly usable interface, which allowed ample configuration and extremely thorough scanning. This resulted in the usual rather slow scanning times, particularly when archive scanning on access was activated against the strong recommendations of the developers – most users would have no requirement for such a level of scanning, but results are recorded here for fairness of comparison against those products which have such scanning enabled by default.

Detection rates were as strong as ever, with some excellent scores in the trojan and RAP sets, again with a fairly clear drop in the 'week +1' set, but the product offers some additional protection features including a cloud-based reputation system, which would doubtless add considerably to its protection capabilities when fully operational. Even without these extras, WildList detection was flawless and no false positives were raised in the clean sets, thus *F-Secure* ably achieves a VB100 award.

G DATA AntiVirus 19.2.0.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.69%
Worms & bots	100.00%	**False positives**	0

G DATA's multi-engine product, combining the strengths of a pair of high-performing detection engines, is another

Archive scanning		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	Ren*
Agnitum Outpost	OD	X	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
AhnLab V3	OD	√	√	√	√	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast!	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√	√
Authentium Command	OD	X	5	5	√	5	2	5	5	√
	OA	X	X	X	X	X	X	X	4	X
AVG	OD	X	√	√	√	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender	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	√	√	√	√	√	8	√	8	√
CA AV	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	X	√
CA eTrust	OD	X	X	1	X	X	X	1	X	√
	OA	X	X	1	X	X	X	1	X	√
Check Point Zone Alarm	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
eEye Blink	OD	X	X	1	1	1	2/8	2	√	√
	OA	X	X	X	X	X	X	X	X	√
ESET NOD32	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
Filseclab Twister	OD	5/√	2/√	4/√	1	4/√	X	5/√	2/√	√
	OA	X	X	X	X	1	X	2	X	X
Finport Simple	OD	X	√	√	X	√	X	√	X	√
	OA	X	√	√	X	√	X	√	X	X
Fortinet FortiClient	OD	X	√	√	√	√	√	4	√	√
	OA	X	√	√	√	√	√	4	√	√
Frisk F-PROT	OD	1	√	√	√	√	√	√	√	√
	OA	1	X	2	X	X	X	2	2	√
F-Secure Client Security	OD	X	5	5	5	X	5	5	5	√
	OA	X/10	X/5	X/5	X/5	X/5	X/2	X/5	X/5	X/√
G DATA	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	OD	√	√	√	√	√	√	√	√	√
	OA	X/4	X/4	X/4	X/4	X/5	X/1	X/2	X/1	√
Kingsoft (Standard)	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
Kingsoft (Advanced)	OD	X	√	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Microsoft Forefront	OD	X	X	X	X	X	X	1	1	√
	OA	X	X	X	X	X	X	1	1	√
Microsoft OneCare	OD	X	X	X	X	X	X	1	1	√
	OA	X	X	X	X	X	X	1	1	√
MWTI eScan	OD	√	√	√	√	√	8	√	8	√
	OA	√	√	√	√	√	8	√	8	√
Norman Security Suite	OD	X	X	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
PC Tools AV	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
PC Tools IS	OD	2	√	√	X	√	√	√	√	√
	OA	2	√	√	X	√	5	√	√	√
PC Tools SD	OD	2	√	√	X	√	√	√	√	√
	OA	2	√	√	X	√	5	√	√	√
Quick Heal	OD	X/2	X/5	2/5	X	2/5	X	2/5	X	X/√
	OA	X	X	X	X	X	X	X	X	X
Redstone RedProtect	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Rising IS	OD	1	√	√	√	√	√	√	√	√
	OA	1	√	√	√	√	√	√	√	√
Sophos Endpoint	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	OD	X	3/10	3/10	3/10	3/10	1/5	3/10	3/10	√
	OA	X	X	X	X	X	X	X	X	√
Trustport	OD	X	√	√	X	√	√	√	√	√
	OA	X	√	√	X	√	√	√	√	√
VirusBuster	OD	2	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot	OD	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	√

Key:

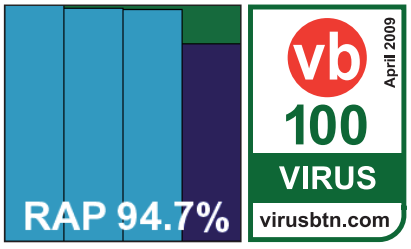
X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

*Executable file with randomly chosen extension

X/√ - Default settings/thorough settings

[1-9] - Archives scanned to limited depth



product which is regularly seen at the top of detection charts in numerous tests, and has an excellent record in our own testing. The latest edition proved quick and simple to install, although it did require a reboot to complete the process, and presented a pleasant and usable interface with a good level of configuration available. Scanning speeds were a little below average, thanks to the multi-engine approach, but the product powered through the infected test sets with no stability problems.

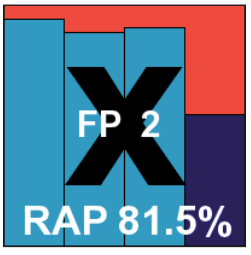
Logging proved a little awkward for our purposes but would probably suit most every-day applications of the product. Detection rates were really quite breathtaking, with over 99% in the trojan set and similarly high scores in most of the RAP sets. Although a slight drop was observed week on week, to a lower level in the 'week +1' RAP set, detection remained highly commendable even here. Attaining a new high in the RAP average scores, and with flawless performance elsewhere, *G DATA* takes maximum honours and an easy VB100 award.

K7 Total Security 9 Desktop 9.7.0200

ItW	100.00%
ItW (o/a)	100.00%
Worms & bots	99.81%
Polymorphic	74.94%
Trojans	91.28%
False positives	2

K7 has been a sporadic entrant in the VB100 testing, putting in strong performances on the occasions it has taken part, but missing a lot of tests – which puts the company at something of

a disadvantage when it comes to keeping up with additions to our clean test sets.



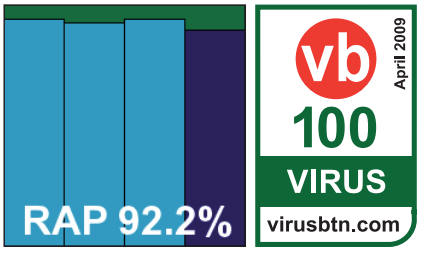
The installation process for the latest product version is fairly smooth, but requires identification details for the user, including email address, as well as a reboot before it can complete – it also offers to remove conflicting third-party software.

The main product interface, once up and running, seemed somewhat cluttered, but offered a good level of configuration and was easy to navigate and use. Detection rates were really quite excellent, with scores above 90% in the key trojan set and in several of the RAP weekly sets (a less spectacular performance in the 'week +1' set brought the overall average down to a still very respectable 81.5%). The product also includes a firewall and privacy guard for added protection.

The WildList was fully covered without issues, but in the clean sets, as feared, a couple of items were flagged as malicious. These were items included on a CD distributed widely in the UK (admittedly somewhat outside of the product's core market regions) by *AOL* in the summer of 2008, and which have been sitting in our clean sets ever since. They were flagged as the Sohanad worm and as an AutoIt trojan, thus spoiling *K7*'s chances of VB100 certification this time despite an otherwise splendid performance.

Kaspersky Anti-Virus 2009 8.0.0.506

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.08%
Worms & bots	100.00%	**False positives**	0



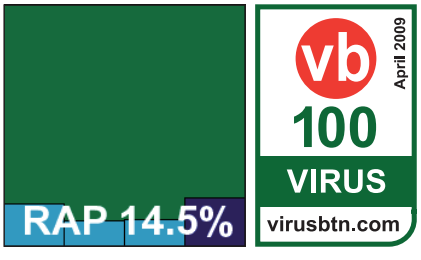
Kaspersky's latest product version is an attractive beast, with a number of added layers of security beyond the standard anti-malware tested here. The installation process includes a data-gathering wizard design to optimize the performance of these various sub-components. This is followed by a reboot to complete the installation.

The new design is very usable as well as visually appealing, and provides plenty of options for fine-tuning the protection levels to suit the individual user. Despite some fairly thorough default settings, scanning speeds were pretty good and on-access overheads fairly negligible. Detection rates, as expected after witnessing the performance of some other products using the same engine, were superb. A particularly strong showing in the 'week +1' RAP set is indicative of some strong heuristics at work in addition to the standard engine that is provided to other products. With an overall RAP average above 90%, *Kaspersky* joins the elite group of top performers, and flawless performances in the WildList and clean sets also earn it VB100 certification once again.

Kingsoft Internet Security 2009 Standard Edition 2008.11.6.63

ItW	100.00%	**Polymorphic**	48.30%
ItW (o/a)	100.00%	**Trojans**	11.97%
Worms & bots	99.27%	**False positives**	0

Kingsoft chose to enter two versions of its product this month, the first of which is a 'budget' edition which lacks some of the more advanced detection features. Although on the surface there are few indications of any difference between the two, some notable variations in performance were observed in several aspects of testing.

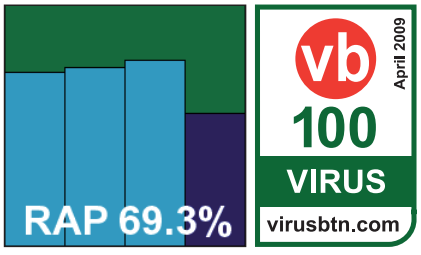


The installation process included a line in the EULA stating that 'basic information about usage' would be collected by the product and passed on to its masters, and also provided a selection box for which the only selection available was 'typical install'. On a few occasions blocks of text seemed to tail off from the installer incomplete, probably due to the integration of translations into the interface.

Scanning speeds were remarkably slow, and overheads similarly intrusive, while detection rates were generally somewhat disappointing, apparently due to a lack of complete functionality in this near-free edition. The WildList was covered without issues however, and there were no false positives in the clean sets, thus earning *Kingsoft* a VB100 award.

Kingsoft Internet Security 2009 Advanced Edition 2008.11.6.63

ItW	100.0%	**Polymorphic**	52.00%
ItW (o/a)	100.00%	**Trojans**	74.05%
Worms & bots	98.84%	**False positives**	0

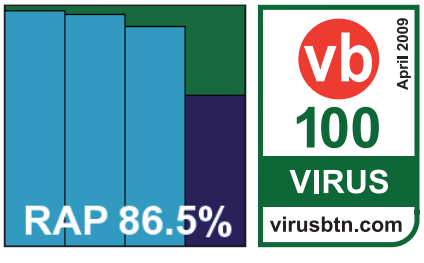


The 'Advanced' or premium version of the *Kingsoft* suite product ran through an identical installation process to that of the basic version, and presented an apparently identical interface. This time, however, scanning speeds were much more impressive. Detection rates also seemed considerably better on first run, causing us to return to the first product for a retry to ensure no logging errors had gone unnoticed – but it appeared that the disparity in detection rates and speeds is entirely due to the additional power of this premium edition.

Again doing well in the core certification requirements, *Kingsoft*'s second product has also done enough to achieve a VB100 award this month.

McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.45%
Worms & bots	100.00%	**False positives**	0



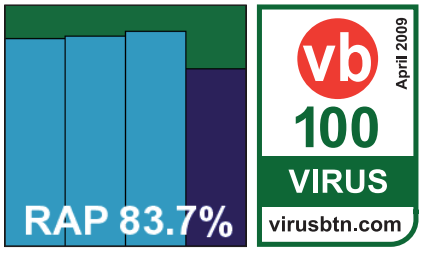
McAfee's corporate product continues to stick to its tried-and-trusted approach, with a very professional and businesslike implementation which won approval from the test team. Setup and configuration for the tests thus proved a joy rather than a chore, and testing chugged through nicely.

Speeds and overheads were both mid-range and fairly unexceptional, but detection rates were excellent in the main, with a notable drop in the 'week +1' RAP set denting the overall RAP average somewhat but still leaving a very respectable 86.5%. Real-world users would have the option of using *McAfee*'s new cloud-based 'Artemis' technology for additional protection from the latest threats, as well as other features including buffer overflow protection.

The sterling work put in across the test sets was carried over to the WildList set and the clean sets, and with nothing to mar an excellent performance VB100 certification is well earned.

Microsoft Forefront Client Security 1.5.1.1955.0

ItW	100.00%	**Polymorphic**	95.09%
ItW (o/a)	100.00%	**Trojans**	84.80%
Worms & bots	100.00%	**False positives**	0



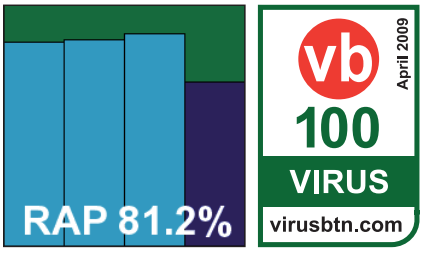
Microsoft's corporate desktop product required a later version of a standard dll before it could install, as our test systems had not been updated since the service pack. This was the only product under test to need such manual adjustments to the environment. With the adjustment made, setup was quite straightforward, and the product proved fairly simple to use, thanks in part to a minimal level of configuration available to the user.

While scanning speeds were reasonable, on-access overheads were fairly high, particularly on executable files, and our test team noticed fairly intrusive slowdowns on the system at several stages during testing.

Detection rates were fairly solid however, and pretty even across the sets, with a much less marked drop in the 'week +1' set than many solutions. With the WildList handled without issues and no false positives, *Forefront* earns itself another VB100 award.

Microsoft Windows Live OneCare 2.5.2900.20

ItW	100.00%	**Polymorphic**	95.09%
ItW (o/a)	100.00%	**Trojans**	83.35%
Worms & bots	100.00%	**False positives**	0



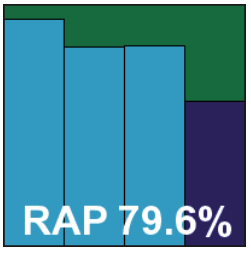
The home-user sibling of *Forefront* proved somewhat simpler to install, with a custom setup process provided to deal with our unconnected environment. The minimal user configuration, absence of progress data and marked system slowdown all made testing rather frustrating. Even worse was the failure of the logging system, which repeatedly refused to generate the 'support log' required to render detection data manageable. On-access scanning of large infected

test sets seemed too much for the product to handle on several occasions, and on a couple of occasions we found the test machine had simply shut down in the middle of a scan (although some suspected hardware issues may have contributed to this issue). On a third attempt at installing and running the product we finally managed to get usable reports, and detection proved much on a par with *Forefront*.

The WildList and clean set provided no unexpected surprises, and *OneCare* thus qualifies for VB100 certification; the team eagerly await its retirement and a more tester-friendly setup in the replacement free version *Morro* due to be made available in the latter half of this year.

MWTI eScan Protection Center 10.0.962.360

ItW	99.01%	**Polymorphic**	100.00%
ItW (o/a)	99.01%	**Trojans**	95.11%
Worms & bots	100.00%	**False positives**	0



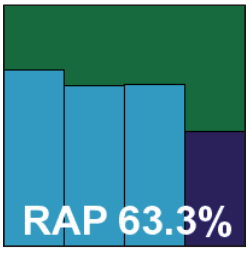
MicroWorld's *eScan* went through a standalone review recently (see *VB*, January 2009, p.16) and was found to be extremely well designed with some excellent additional protection features, the configuration of which is a glowing example of user-friendliness. This latest update was found to be visually appealing by the test team, with a fast installation process that includes a pre-install scan, but which requires a reboot to complete. Default settings are fairly thorough, which is reflected in rather sluggish scanning speeds and fairly hefty on-access overheads.

Previous editions of the product included the *Kaspersky* detection engine alongside various items of in-house technology, but the firm announced a few months ago that its latest range would include entirely in-house engines – a bold move. With the new setup, detection rates were very solid across most of the test sets, with some excellent figures in the trojan and RAP sets, although rates declined somewhat over the very newest items. With all the additional HIPS technology included in the product, the protection provided against threat vectors in the real world would, of course, be increased.

The product encountered no problems in the clean sets, but in the WildList set a couple of the recent additions to the list were missed, showing some minor teething problems for what looks likely to be a strong new detection engine. No VB100 award is forthcoming this month, but *MWTI* looks likely to be back on track very soon.

Norman Security Suite 7.10

ItW	99.79%	**Polymorphic**	83.21%
ItW (o/a)	99.79%	**Trojans**	81.14%
Worms & bots	100.00%	**False positives**	0



Norman's product has undergone a significant facelift of late, but despite a speedy installation process the new look did not go down well with the test team, who found it rather peculiar to look at, very short on options, and difficult to navigate. There appeared to be no option to run on-demand scans from the interface, and the scheduler system seemed not to be working for us, so on-demand tests were run using the right-click scan option.

This produced some fairly slow scan times on demand, thanks to the intensive sandbox technology, but on-access overheads were pretty light. After running some of the detection tests the product ran into some difficulties, in which the right-click option vanished and protection was apparently disabled; even the protection area of the interface appeared to have vanished without trace. Logging of the tests carried out thus far showed results well short of the expected level. With no response from any attempt to revive it, and even a reboot proving inadequate, a fresh install was required to complete the testing.

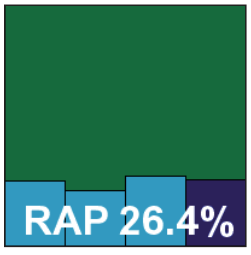
On second attempt things went a little better, with some much more stable behaviour getting us far enough to acquire and process full detection logs. The logs showed detection figures that were pretty much in line with previous performances, before the mysterious shutdown occurred once again. Analysis of the results showed some pretty decent scores in the trojan set, with a gradual decline across the RAP sets to a fairly low level in the 'week +1' set. Elsewhere, the W32/Fujacks samples in the WildList set were missed, and so *Norman* does not make the grade for a VB100 award this month.

PC Tools Anti-Virus 2009 6.0.0.16

ItW	99.75%	**Polymorphic**	18.55%
ItW (o/a)	99.75%	**Trojans**	22.32%
Worms & bots	99.81%	**False positives**	0

The *PC Tools* product lines have caused us some difficulties in the past, as much thanks to their oddities of behaviour and design as to a tendency for more than one version to be submitted. This month, three products were submitted, of which we were told that the simple AV solution was

considered the lowest priority by the vendor, should any have to be excluded from the test due to time constraints.



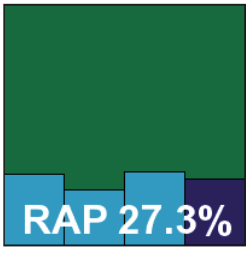
It also proved somewhat simpler to test than the others in the range, with a speedy and simple installation process after which no reboot was required. The interface provides minimal configuration and has a few peculiarities of layout which makes the options that are available less than easy to find. However, it seemed to work reasonably well in the on-access tests over clean and archive sets.

Attempting to run the same test over the infected sets appeared to go smoothly at first, but halfway through protection seemed to shut down and blocking access to infected items ceased; they were no longer logged either. After several attempts at the test, including slowing down the rate of file access, we eventually managed to coax what appeared to be usable results from the product, although the periodic shutdowns continued. On demand tests were less tricky, although the results found in the logs, particularly for the RAP sets, were much lower than expected. In the WildList, the W32/Fujacks set of samples were not detected, with an additional file missed on access only, and as a result *PC Tools* does not earn a VB100 for its AV product this month.

PC Tools Internet Security 6.0.1.440

ItW	99.75%	**Polymorphic**	18.55%
ItW (o/a)	99.75%	**Trojans**	22.79%
Worms & bots	99.85%	**False positives**	0

The second *PC Tools* product, the *Internet Security* suite, combines the anti-malware protection of the company's flagship *Spyware Doctor* product with some additional protection measures, including a firewall.



Installation, which includes the offer of a *Google* toolbar along with the product itself, seemed fairly straightforward until the product was up and running, at which point it was immediately clear that something was not right – all status alert records were marked 'off' or 'checking', and on-access detection was clearly not present. Upon consulting with the developers, we were informed of some recently discovered issues with our rather unusual hardware setup, which should have been resolved by a simple reboot – but this proved ineffective. Eventually, we managed to persuade the product to switch itself on by connecting it to the Internet, with updates disabled; within a few seconds it all came online. This kind of thing is not uncommon these days, but is something of a problem for many users. Although I may be somewhat atypical and overly paranoid, I like to ensure that a new system is fully protected and even up to date before I expose it to the Internet, so always use offline installers and updaters where possible when building a new machine or reimaging from a known safe state – being forced to go online to activate a product is of no interest to me. However, many products seem to want to do such things to prevent piracy or for other reasons best known to them.

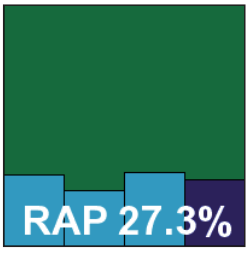
With the product finally activated, we ran through the tests. In this product, on-access scanning is not activated by simple file access, so once again we had to resort to copying test sets across the network and trusting the product's logging to show us if it suffered similar shutdowns to the previous version. Logging, of both on-access and on-demand data, proved less than helpful, regularly imposing apparently random cut-off points, though it was not always clear if this was the protection or the log that had ceased to record new arrivals. Eventually, after much sweating and cursing from the team, we managed to obtain usable data, which fairly closely matched that of the previous product, leading us to believe that both must be representative of the protection offered.

On-demand scanning speeds were rather slow, particularly over the archive set, and while on-access times could not be recorded using our standard methods, it was obvious that the systems were much less responsive, and the product interface itself proved especially slow to respond. Detection results were not great, and the W32/Fujacks samples in the WildList set put paid to *PC Tools*' hopes of certification for this product too.

PC Tools Spyware Doctor with Anti-Virus 6.0.1.440

ItW	99.75%	**Polymorphic**	18.55%
ItW (o/a)	99.75%	**Trojans**	22.79%
Worms & bots	99.85%	**False positives**	0

The third and final *PC Tools* product proved almost identical to the suite product, minus the firewall, and provided the same sort of agonies for the test team, including the need to connect to the web to get it to turn anything on. After repeated attempts and numerous apparent brick walls, some sort of results emerged from the confusion, proving

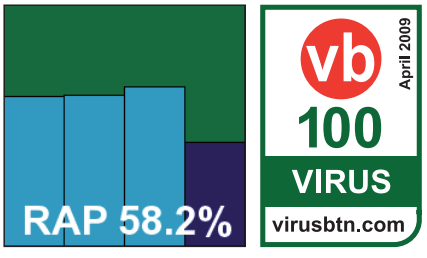


pretty much identical to the suite product right down to the WildList misses and failure to qualify for certification.

Due to the numerous problems with the products, not least the unreliable logging features, it is more than possible that the results recorded here do not show the full detection capabilities of the product range, but they are at least an approximation of the best detection that could be coaxed from the product over several arduous days of repeated tests.

Quick Heal Anti-Virus Lite 2009

ItW	100.00%	**Polymorphic**	95.09%
ItW (o/a)	100.00%	**Trojans**	86.61%
Worms & bots	99.32%	**False positives**	0



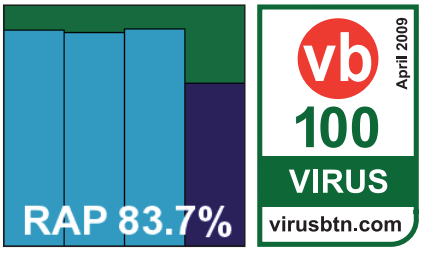
As usual, *Quick Heal*'s product lived up to its name with a very rapid installation process and no reboot necessary. The interface was perhaps a little confusing, with some of the options hidden away in unexpected places, but it generally proved usable and responsive with no stability issues.

Scanning speeds were, as expected, remarkably quick, and on-access overheads extremely light. Detection across the test sets was fairly average, with a pretty marked drop in the 'week +1' RAP set, but the product does include additional features, including some advanced static heuristics based on file locations and names which would not be reflected by our testing methodology.

In the core areas of the WildList and clean sets there were no problems however, and *Quick Heal* duly earns a VB100 award.

Redstone RedProtect 1.7.5

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.16%
Worms & bots	100.00%	**False positives**	0



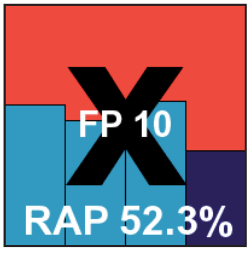
Redstone's product is a rather unusual one, designed to be managed entirely remotely with little user interaction. The installation process, which is dependent on the .NET framework, was thus custom-tweaked for our purposes, and access to configuration was also provided via a custom interface. Both were fast and simple to use, and highly rated by the test team for usability.

The 'default' settings provided for us were thorough, resulting in below-average scanning speeds, but overheads were not too intrusive.

Detection rates from the *Kaspersky* engine were as excellent as we would expect, although a notable drop over that tricky 'week +1' RAP set indicated that some aspects of *Kaspersky*'s detection abilities are not included here. With the WildList set covered flawlessly, and no problems in the clean sets, *Redstone* comfortably earns a VB100 award.

Rising Internet Security 21.27.10

ItW	99.75%	**Polymorphic**	70.02%
ItW (o/a)	99.75%	**Trojans**	56.71%
Worms & bots	99.18%	**False positives**	10



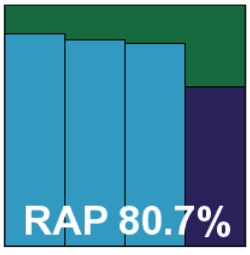
Rising's product is another to have been reviewed in depth recently (see *VB*, March 2009, p.13), and full details of the setup process (rather complex, with a reboot and several post-install wizards) and additional features (which include a dancing lion cartoon and a range of firewall and basic HIPS technologies) are covered in more depth there.

In this case we mostly looked at scanning speeds and detection rates. Despite some very thorough default settings which covered most of our archive sets in full depth, on-demand scanning was fairly rapid, while on-access scanning is only available on write or on execute and thus could not be fitted into our standard overhead measurement.

Detection results were gathered by copying test sets to the system across the network, and proved fairly mediocre across the board. In the clean sets, a smattering of false positives were raised, and in the WildList set a single W32/Autorun variant was not detected, and as a result *Rising* will have to wait a little longer for its next VB100 award.

Sophos Endpoint Security and Control 8.0 (7.64)

ItW	100.00%	**Polymorphic**	89.25%
ItW (o/a)	100.00%	**Trojans**	83.49%
Worms & bots	100.00%	**False positives**	0



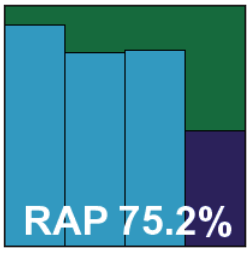
The *Sophos* product proved very smooth and quick to install, and was another one of the select few that offered to remove conflicting third-party software. No reboot was required.

The interface is clear and simple, with a great deal of configuration tucked away under the bonnet, as befits the product's corporate target market. On-demand scanning speeds were pretty decent, and on-access overheads not too intrusive, at least with the sensible default settings. Detection rates were solid and respectable across the sets, with a fairly notable drop in the unknown 'week +1' samples.

The WildList presented no issues, and in the clean sets only a couple of suspicious alerts were raised (on files which turned out to be of rather peculiar makeup). A VB100 award is thus earned by *Sophos*.

Symantec Endpoint Protection 11.0.4010.19

ItW	100.00%	**Polymorphic**	99.96%
ItW (o/a)	100.00%	**Trojans**	91.49%
Worms & bots	100.00%	**False positives**	0



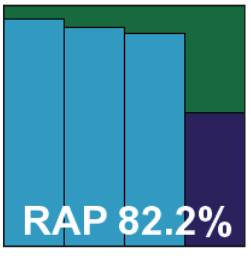
Symantec's corporate desktop product, previously much praised for its plain and businesslike style, has become a lot more glossy and colourful of late, but remains grey and serious in the deeper configuration areas. Installation is pretty simple, and navigation of the interface is reasonably sensible, with the configuration pages, once dug out, providing a fair level of control over the product's behaviour.

Scanning speeds were fairly middling, but on-access overheads were not bad at all, and testing thus progressed fairly rapidly. When scanning the infected sets, the machine shut down unexpectedly during one of the on-access tests, and on another occasion the interface suffered a crash, although protection remained in place.

Detection rates proved pretty decent, although the 'week +1' drop was fairly sharp. With no problems encountered in the WildList test set and no false positives in the clean set, *Symantec* takes another VB100 in its stride.

Trustport Anti-Virus 2009 2.8.0.3012

ItW	99.79%	**Polymorphic**	98.56%
ItW (o/a)	99.79%	**Trojans**	94.50%
Worms & bots	100.00%	**False positives**	0

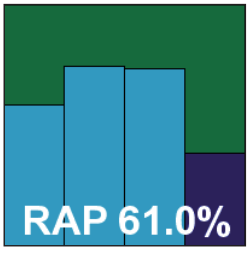


Trustport's multi-engine approach has achieved some superb scores in some recent tests, although frequent changes to the combination of engines included have led to some less distinguished performances too. The latest version offers a fast and simple installation, with some new adornments to what is essentially the same interface, currently using the *Norman* and *AVG* engines under the covers.

With some very thorough defaults on top of the multi-engine design, scanning speeds are understandably rather slow, and on-access overheads also rather heavy, but detection rates were generally pretty good. Scores above 90% were achieved in the trojan set and some of the RAP sets, but the 'week +1' set showed a fairly steep decline. Oddly, a few items including the W32/Fujacks replicants were not detected in the WildList set – suggesting that slightly outdated detection data may have been in use. As a result, *Trustport* is denied a VB100 award this time.

VirusBuster Professional 5.003 b.155

ItW	100.00%	**Polymorphic**	88.85%
ItW (o/a)	100.00%	**Trojans**	69.71%
Worms & bots	99.92%	**False positives**	0



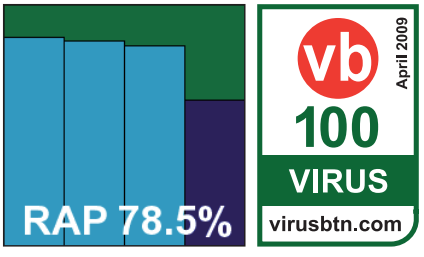
VirusBuster's product is another which has remained little changed over several years of testing, and our test engineer remarked on some awkwardness in the otherwise speedy installation, as well as a rather unintuitive main interface. However, with the help of some experience to navigate its peculiarities, testing proceeded, with some good scanning speeds in both modes helping things along.

Detection rates were somewhat below average, with a particularly sharp drop in the 'week +1' RAP set, but

elsewhere things were a little more respectable, and with no problems in the WildList and no false positives, *VirusBuster* earns another VB100 certification.

Webroot Anti-Virus with Anti-Spyware

ItW	100.00%	**Polymorphic**	89.16%
ItW (o/a)	100.00%	**Trojans**	82.50%
Worms & bots	100.00%	**False positives**	0



Webroot's product has undergone some name changes but seems little changed in layout since the company's first entry. The installation went smoothly thanks to some well-documented additional steps required to fit in with our lab setup, but the interface proved highly unpopular with the lab team, who remarked on its awkward and unintuitive layout, the difficulty of finding the few options available, and also some extremely slow response times to fairly simple button clicks. Other areas where bad behaviour was noted included logging, which was regularly truncated and barely usable in some cases, and on-detection actions, which were often performed despite specific instructions to do nothing.

Eventually, after much hair-tugging, results were obtained, and proved much in line with the *Sophos* engine underlying the product. With no false positives and nothing missed in the WildList set, *Webroot* earns the final VB100 award of this month's test.

CONCLUSIONS

This month's test has presented the usual ups and downs, with some truly excellent products and some real horrors. The first full-scale rollout of our RAP tests has provided some interesting data on the whole, with several products excelling and a few failing to impress. Many products showed a gradual week-on-week decrease in detection rates, which is as predicted and goes some way to validating the test methodology. The severity of the final week drop in detection is perhaps the most telling part of the results, indicating how well heuristic and generic detection is working.

In a couple of cases, where products integrate engines bought in from outside, the results have shown how well some OEMs are adding their own technology to what they have bought in, while in one case the OEM has done less well than the original engine maker in the vital heuristic area.

In the standard areas of the test, a pretty good month was had by most, with a large number of VB100 awards having been handed out. A smattering of false positives ran through a number of products, most of which were caused by the batch of files from a UK *AOL* CD hitting Asian-focused products. As mentioned, we have been trying to work on ways of ensuring our clean sets are kept relevant, and are hoping to introduce some more advanced classification and ranking of clean files at some point. The issue raised here though – that of the locality of clean samples, where samples likely only seen in one specific region have spoiled the chances of products that are focused on an entirely different region – is less simple to solve. Our testing aims to present a global picture, and so our detection standards – both for infected and clean files – must try to reflect the global landscape of malware and software. While we cannot ignore the effects of files from one region on products from another, we can (and do) make efforts to ensure our test sets fairly reflect all regions.

Another major headache this month has been product stability issues, something that has been raised here in several recent tests. In a number of cases it has left our lab techs astounded to see how fragile and unstable some software can be – particularly considering it is supposed to be protecting systems from danger. Some of our advisors have even suggested automatically failing any product which crashes – something we will certainly have to consider when we next update the test procedures.

This month saw a smattering of misses in the WildList, most notably a small number of fairly simple file infectors. We have seen similar incidents before and hope they encourage analysts to ensure that file infectors continue to be handled properly, and not lost in the floods of static samples pouring into labs. The next test (which will take place in May on the *Windows Server 2003* platform) should see some much more tricky polymorphic items making their way onto the WildList, and we look forward to the challenge this will pose for the products on test.

Technical details

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

Any developers interested in submitting products for VB's comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.