

COMPARATIVE REVIEW

VB100 – WINDOWS VISTA BUSINESS EDITION SERVICE PACK 2

John Hawes

Yes, I know. *Windows Vista*. Not the most lovable of platforms. It was released to a barrage of bad press, faced all kinds of criticisms, from slowness to insecurity to downright ugliness, and wasn't really considered reliable until the release of service pack 2 – by which time *Windows 7* was on the horizon promising more of the same only better. The VB test team had entertained vague hopes that, once *Windows 7* was out, we might be spared the trauma of another *Vista* test, but considering the surprisingly large user base still maintained by the now outmoded operating system (estimates are that it still runs on over 20% of systems), it seemed a little premature to give up on it entirely. So, this may be one last hurrah for a platform that has caused us much grief and aggravation in the past.

After the massive popularity of the last desktop comparative (see VB, April 2010, p.23) we expected another monster haul of products, and sure enough the submissions came flooding in. Although not quite breaking the record, this month's selection of products is still remarkably large and diverse, with the majority of the familiar old names taking part and a sprinkling of newcomers to provide some extra interest. Given what seems like a new, much higher baseline, we may have to consider revising our rules for free entry to these tests – as the situation currently stands, any vendor may submit up to two products to any single test without charge, and a small fee is levied on third and subsequent entries. This month only one vendor chose to submit more than two products, but in future it may become necessary to impose charges on any vendor submitting more than one product – which would at least provide us with extra funds for hardware and other resources involved in running these tests, and possibly allow us some time and space to work on new, more advanced testing.

PLATFORM AND TEST SETS

Setting up of *Vista* is actually a fairly painless process these days, with the install media used including SP2 from the off and thus skirting round some of the problems encountered in our first few exposures to the platform. The installation process is reasonably simple, with just a little disk partitioning and so on required to fit in with our needs. Once up and running, no additional drivers were required to work with our new batch of test systems; after installing a few handy tools such as archivers and PDF viewers, and

setting the networking and desktop layouts to our liking, images were taken and the machines were ready to go.

Several of the products entered this month required Internet access to update or activate. These were installed in advance, allowed to go online to do their business, and then fresh images were taken for later use. Test sets were then copied to the test machines.

This month's core certification set was synchronized with the June 2010 WildList, which was released a few days prior to our official test set deadline of 24 July. The list was once again fairly unspectacular, with the bulk of the contents made up of social networking and online gaming data stealers. Of most note, perhaps, were three new strains of W32/Virut, the complex polymorphic virus which has been the bane of many a product over the last few years. These three were replicated in reasonably large numbers to ensure a thorough workout for the products' detection routines; one of the three proved more tricky to replicate than the others, and credit is due to the lab team for getting our prototype automated replication system running in a way which could persuade it to infect a large enough set of samples for our needs. Including a few thousand samples of each polymorphic virus on the list, the WildList test set contained some 9,118 unique samples.

The other side of the certification requirements, the clean set, was updated and expanded as usual, with large swathes of new packages and package versions gathered from the most popular items on leading download sites, as well as additional items from CDs, DVDs and other media obtained by the lab in recent months. Among the items added were a number of tools related to television and other media-viewing hardware, and also quite a lot of items connected to document manipulation. In all, after a purging of some older and less relevant items, the clean set came in at close to 400,000 unique files.

The speed sets were left pretty much unchanged from previous tests, and the measures of RAM and CPU usage we have been reporting recently were recorded as before. The other detection test sets were compiled as usual, with the RAP sets put together from significant items gathered in the three weeks leading up to the 24 July product deadline and the week following, and the trojans and worms & bots sets bulked up with new items received in the month or so between RAP sets. With further expansion of our sample-gathering efforts the initial numbers were fairly high, but every effort was made to classify and validate as much as possible prior to the start of testing, to keep scan times to a minimum. Further validation continued during testing and items not meeting our requirements were struck from the sets; in the end, the weekly RAP sets contained around 10,000 samples per week, with just over 70,000 in

the trojans set and 15,000 in the worms and bots set. The polymorphic set remained largely the same as in previous tests, with the main addition being some older Virut strains which have fallen off the WildList of late, in expanded numbers.

One other addition was made, to the set of samples used to measure archive scanning. This was enlarged slightly to include zipx format, a new and improved version of zip archiving used by the latest version of *WinZip*. We also included self-extracting executable archives compressed using the rar format. These samples are produced by adding the Eicar test file and a clean control file to an archive of each type. The first level archives are then added, along with another clean control file, to another archive of the same type to make the level 2 sample, and so on. The purpose of these is to provide some insight into how deeply each product analyses various types of compressed files, to help with comprehension of the speed results we report. Thus, if a product has a slow scanning speed but delves deeply into a wide range of archive types, its times and lags should not be directly compared with a product which analyses files less deeply. Another copy of the Eicar file is included in the test set uncompressed but with a randomly selected, non-executable extension, to show which products are relying on extension lists to determine what is scanned. This may have some effect on speeds over the other speed sets, notably the 'media & documents' and 'other file types' sets, which may include many files without standard executable extensions.

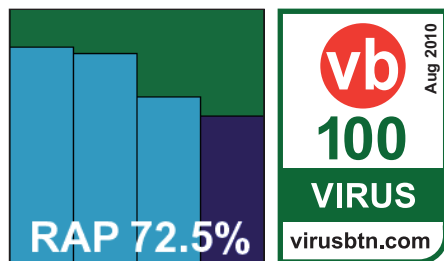
With all this copied to the secondary hard drives of the lab systems, we were ready to get down to some testing.

Agnitum Outpost Security Suite Pro 7.0.1 (3376.514.1234)

ItW	100.00%	Polymorphic	89.73%
ItW (o/a)	100.00%	Trojans	82.07%
Worms & bots	91.12%	False positives	0

Agnitum's Outpost is a fairly thorough suite solution which includes the company's renowned firewall, an anti-malware component

based around the *VirusBuster* detection engine, some proactive protection, web content filtering, spam blocking and more. Of course, only a subset of the protection



provided by the suite is properly measured here. As a result of the defence in depth offered, running the 99MB pre-updated install package leads to an installation process which has rather more than the usual number of steps and takes a few minutes to get through; at the end a reboot is required to get everything settled into place, and on initial boot-up the system took a little longer than usual to return control as the various components were activated.

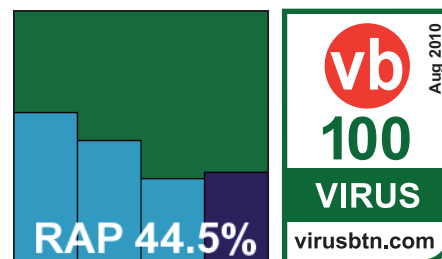
When we finally got access to the main interface we noted it looked slightly refreshed, with a more curvy and shiny feel, though much of this could have been the impact of *Vista's* own shininess. We have long been fans of the simple and businesslike design and layout of the *Agnitum* GUI and it has lost none of its efficiency and solidity. With so many components here to control, the anti-malware configuration is fairly basic but offers the standard options in a lucid and logical style. Some caching of data meant that scanning of previously checked files was very speedy and although initial scanning speeds were medium, the 'warm' measures were much more impressive. RAM usage remained fairly steady – at the upper end of the middle of the scale – regardless of whether file access was taking place, with CPU usage similarly placed against other products in this month's test.

We noted that the product appeared not to be looking inside the new zipx format archives, though it was not clear whether this was down to a lack of ability to decompress the format or the product merely not yet recognizing the extension as an archive type. Detection rates across the standard sets were respectable, and RAP scores started fairly respectably for older items, falling off fairly sharply in the newer sets. No problems were encountered in the clean or WildList sets, and *Agnitum* gets this month's comparative off to a good start with a well-earned VB100 award.

AhnLab V3 Internet Security 8.0.3.7 build 372

ItW	100.00%	Polymorphic	99.84%
ItW (o/a)	100.00%	Trojans	63.71%
Worms & bots	78.54%	False positives	0

AhnLab also provided an installer with the latest updates included, measuring just over 96MB, but this time the installation process was much faster and simpler. Only the basic



On-demand tests	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	1452	91.12%	192	89.73%	12789	82.07%		11
AhnLab V3	0	100.00%	3508	78.54%	7	99.84%	25893	63.71%		
Avast! Free	0	100.00%	539	96.70%	522	93.71%	3896	94.54%		1
AVG IS	0	100.00%	1008	93.83%	53	97.86%	1781	97.50%		
Avira AntiVir	0	100.00%	215	98.68%	0	100.00%	1833	97.43%		
BitDefender	0	100.00%	249	98.48%	0	100.00%	13303	81.35%	15	
Bkis Gateway	0	100.00%	6205	62.04%	1601	64.53%	46176	35.28%		
Bkis Home	0	100.00%	6204	62.05%	3362	56.10%	46176	35.28%		
Bkis Pro	0	100.00%	6204	62.05%	1601	64.53%	46176	35.28%		
CA ISS Plus	5	99.18%	2227	86.38%	3469	92.58%	21493	69.87%		1
CA Threat Manager	1	99.84%	3891	76.20%	3469	92.58%	32219	54.84%		
Central Command Vexira	0	100.00%	1293	92.09%	192	89.73%	12173	82.94%		
Check Point Zone Alarm	0	100.00%	731	95.53%	0	100.00%	6238	91.26%		
Coranti Multicore	0	100.00%	82	99.50%	0	100.00%	380	99.47%	15	
Defenx Security Suite	0	100.00%	1318	91.94%	192	89.73%	12128	83.00%		11
Digital Defender	1	99.84%	1889	88.44%	192	89.73%	13764	80.71%		
eEye Blink	0	100.00%	2396	85.34%	290	84.55%	21385	70.02%	1	
Emsisoft Anti-Malware	0	100.00%	198	98.79%	1371	79.99%	5528	92.25%		1
eScan ISS	1	99.84%	268	98.36%	0	100.00%	1894	97.35%		
ESET NOD32	0	100.00%	204	98.75%	0	100.00%	3964	94.44%		
Filseclab Twister	3191	98.48%	2290	85.99%	14087	41.76%	9827	86.23%	3	
Fortinet FortiClient	0	100.00%	2778	83.01%	30	99.36%	28320	60.30%		
Frisk F-PROT	0	100.00%	1736	89.38%	0	100.00%	15482	78.30%		
F-Secure Client Security	0	100.00%	218	98.67%	0	100.00%	1835	97.43%		
F-Secure PSB	0	100.00%	360	97.80%	0	100.00%	2512	96.48%		
G DATA	0	100.00%	298	98.18%	0	100.00%	1410	98.02%	15	
Ikarus virus.utilities	0	100.00%	212	98.70%	1371	79.99%	6879	90.36%		1

(Please refer to text for full product names)

steps of EULA, licensing, location and component selection were required, and within 30 seconds it was all up and running with no reboot necessary.

The interface seemed to have had some work done on it, looking quite pleasant in the glitzy surroundings of *Vista*, and with configuration controls easier to find and clustered in a more rational and logical fashion. Again, several additional components are provided besides the anti-malware basics, including modules labelled ‘network

protection’, ‘content filtering’, ‘email protection’ and ‘system tuning’. One notable feature of the redesign is an end to the separation of scans for malware and spyware, although these continue to be logged separately.

Running through the performance test took some time, as the on-demand scanner has pretty thorough default settings; scan times were not unreasonable, but a lack of caching of results meant that repeat scans took as long as the first run. RAM usage was fairly low, and CPU drain not too heavy

either, even under heavy stress, but lag times to access files were perhaps just a shade above average. The detection tests also proved somewhat drawn out: the initial on-access run suffered no problems but subsequent on-demand scans were hampered by the repeated appearance of on-access alerts, comprising the last thousand or so detections from the on-access test. These appeared every few minutes, over and over again even after rebooting the system, and were appended repeatedly to logs as well. The heavy toll of this odd behaviour may have contributed to a crash which occurred during one of the main test set scans, and also to the rather long wait for the logging system to export results.

In the end, however, full results were obtained, and the crashing problem was not repeated. We found fairly decent scores in the main test sets, and while *AhnLab*'s scores won't trouble the leaders on the RAP quadrant, they were close to the main pack. Checking the scan results, we were worried at first that a handful of files in the WildList set had been missed on access, but looking more closely at the product's logs showed that the items in question had in fact been detected and logged by the anti-spyware component. This claimed to have blocked access to them but had clearly not done so as thoroughly as the full anti-malware module would have done, as our opener tool was able to access and take details of the files in question. However, as the VB100 rules require only detection and not full blocking of malicious files this did not count against *AhnLab*, and with no false alarms in the clean sets, a VB100 award is duly earned.

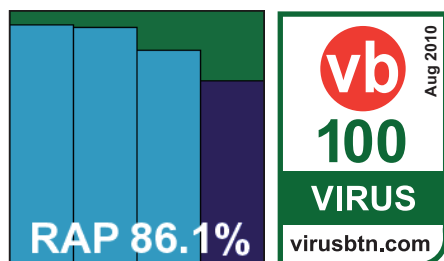
Avast Software avast! Free Antivirus 5.0.545

ItW	100.00%	Polymorphic	93.71%
ItW (o/a)	100.00%	Trojans	94.54%
Worms & bots	96.70%	False positives	0

Enough time has been spent in these pages drooling over the beauty of *Avast*'s latest version; suffice to say that after several appearances in

our tests it has lost none of its lustre. The installer, a mere 51MB with all updates included, runs through in a handful of steps, one of which is the offer to install *Google*'s *Chrome* browser, and is all done in a few seconds with no need to reboot.

The change in the company name is clearly still filtering through, with some of the folders used for the install



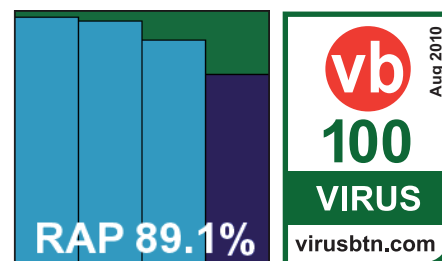
still bearing the old '*Alwil*' name, but the main interface remains glistening, smooth and solid as a rock. On-demand scanning speeds were lightning fast, with no indication of any speed-up in the 'warm' scans but not much room for improvement over the cold times anyway. With feather-light impact on file access, and fairly sparing use of both memory and processor cycles, *Avast* does well in all the performance measures this month.

Detection rates across the sets were also pretty superb, and the WildList and clean sets presented no problems to the product, which brushed everything aside with aplomb. With extra kudos for prettiness, reliability and ease of testing, *Avast* comfortably wins another VB100 award.

AVG Internet Security 9.0.837

ItW	100.00%	Polymorphic	97.86%
ItW (o/a)	100.00%	Trojans	97.50%
Worms & bots	93.83%	False positives	0

AVG's current flagship suite was also provided pre-updated, the installer measuring a fairly hefty 109MB. As another multi-



faceted suite the installation process had several stages, including the offer of a *Yahoo!* toolbar, but was completed within a couple of minutes, ending with information on sending detection data back to base and an 'optimization scan', which was over in a minute or two; no reboot was required.

The product's main interface has a fairly standard layout, which is a little cluttered thanks to the many modules, several of which are not covered by our standard tests. With some pretty thorough default settings on demand, initial scans took quite some time to complete, but judicious ignoring of previously scanned files – of certain types at least – made for some much faster 'warm' runs. File access slowdown was not too heavy, and RAM usage was well below that of the more draining products seen this month, while CPU usage was towards the middle of the scale.

Running through the detection tests was also a mix of fast and slow. One run – in which the scan priority was bumped up to get through the infected sets faster – zipped merrily to what appeared to be the end of the job, then lingered at 'finishing' for several more hours, while the number of

On-demand tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
K7 Total Security	0	100.00%	1012	93.81%	0	100.00%	10121	85.81%		
Kaspersky Anti-Virus 6.0	0	100.00%	375	97.71%	0	100.00%	4427	93.79%		
Kaspersky IS 2011	0	100.00%	562	96.56%	0	100.00%	6533	90.84%		
Keniu Antivirus	0	100.00%	568	96.53%	0	100.00%	6297	91.17%		1
Kingsoft IS Advanced	8	99.999%	8554	47.67%	4828	58.88%	60603	15.05%		
Kingsoft IS Standard	8	99.999%	9063	44.56%	4828	58.88%	62622	12.22%		
Lavasoft Ad-Aware Professional	0	100.00%	310	98.10%	1054	73.53%	3637	94.90%		
Lavasoft Ad-Aware Total Security	0	100.00%	288	98.24%	0	100.00%	1276	98.21%	1	
McAfee Total Protection	5	99.9997%	870	94.68%	1	99.999%	9138	87.19%		1
McAfee VirusScan	5	99.9997%	1287	92.13%	1	99.999%	14153	80.16%		
Microsoft Security Essentials	0	100.00%	272	98.34%	0	100.00%	4075	94.29%		
Nifty Security24	0	100.00%	687	95.80%	0	100.00%	8703	87.80%		5
Norman Security Suite	0	100.00%	2413	85.24%	295	84.02%	21513	69.85%	1	
PC Tools IS	0	100.00%	1816	88.89%	0	100.00%	14063	80.29%		
PC Tools Spyware Doctor	0	100.00%	1816	88.89%	0	100.00%	14063	80.29%		
Preventon Antivirus	1	99.84%	1889	88.44%	192	89.73%	13764	80.71%		11
Proland Protector Plus	0	100.00%	1444	91.17%	192	89.73%	13639	80.88%		
Qihoo 360	0	100.00%	240	98.53%	0	100.00%	1584	97.78%	15	
Quick Heal AntiVirus	0	100.00%	1620	90.09%	2	99.94%	12971	81.82%		
Returnil RVS	0	100.00%	1613	90.13%	0	100.00%	14621	79.51%		1
Rising IS	0	100.00%	5958	63.55%	3576	70.87%	32096	55.01%	2	
Sophos Endpoint	0	100.00%	1859	88.63%	0	100.00%	8139	88.59%		4
SPAMfighter VIRUSfighter	1	99.84%	1891	88.43%	192	89.73%	13782	80.68%		11
Sunbelt VIPRE	0	100.00%	355	97.83%	1054	73.53%	6775	90.50%		
Symantec Endpoint Security	0	100.00%	2217	86.44%	0	100.00%	16121	77.40%		
Trustport AntiVirus	0	100.00%	214	98.69%	0	100.00%	1180	98.35%		
VirusBuster Professional	0	100.00%	2868	82.46%	192	89.73%	15291	78.57%		

(Please refer to text for full product names)

detections continued to rise; it gave the impression that the 'fast scan' option simply sped up the progress bar, and not the actual scan time at all.

Despite this minor (and rather specialist) issue, everything completed safely and reliably, with some splendid detection rates across the sets, and RAP scores were particularly impressive once again. The WildList and clean sets were handled impeccably, and AVG also earns another VB100 award.

Avira AntiVir Professional 10.0.0.918

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.43%
Worms & bots	98.68%	False positives	0

The paid-for version of Avira's *AntiVir* came as a standard installer package of 46MB with additional updates weighing in at a smidgen under 35MB. The installation process is

made up of the standard selection of stages, plus a screen advising users that they might as well disable *Microsoft's* *Windows*

Defender (although this action is not performed for you). The whole job was done in under a minute and no reboot was needed.

The main interface was another which seemed to have had a bit of a facelift, making it a little slicker-looking than previous versions, although some of the controls remain a little clunky and unintuitive, to us at least. The configuration system offers an 'expert mode' for more advanced users, which more than satisfied our rather demanding requirements, with a wealth of options covering every possible eventuality.

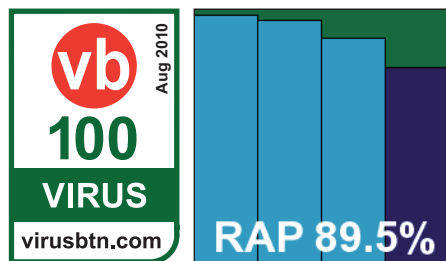
Speed tests tripped through in good time, with no sign of speeding up in the 'warm' scans but little need for it really, and performance measures showed fairly low use of both memory and CPU, with a pretty light touch on access too. Detection rates were as top-notch as ever, with excellent scores across all sets, RAP scores being especially noteworthy. No issues were observed in the WildList or the clean set, and a VB100 award is easily earned.

BitDefender Business Client 11.0.22

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	81.35%
Worms & bots	98.48%	False positives	15

BitDefender's latest corporate solution was delivered to us as a 122MB installer, which ran through the standard set of stages plus a step to disable both *Windows Defender* and the *Windows Firewall* in favour of the product's own protection. The process was pretty speedy, although a reboot was required at the end to fully implement protection.

The interface – making its debut on our test bench – was plain and unflashy, with basic controls on the main start page and an advanced set-up area providing an excellent degree of configurability as befits the more demanding business environment. It all seemed well laid out and



simple to navigate, with everything where it might be expected to be.

Running through some tests, however, showed that there may still be a few minor bugs that need ironing out. The heavy load of the detection tests brought up error messages warning that the 'Threat monitor' component had stopped working. By breaking the tests down into smaller sections we managed to get to the end though, and this problem is unlikely to affect most real-world users who are not in the unfortunate position of being bombarded with tens of thousands of malicious files in a short space of time.

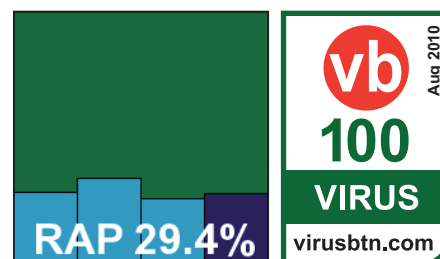
Slightly more frustrating was an apparent problem with the on-demand scan set-up. This allowed multiple folders to be selected for a single scan; on several occasions it reached the end of the scan and reported results, but seemed only to have covered the first folder on the selected list. Again, re-running the tests in smaller chunks got around this issue quite simply.

On-demand scanning speeds were good, although in some of the scans hints of incomplete scanning were again apparent; the media & documents sets were run through in a few seconds, time and time again, but re-scanning different sub-sections produced notably different results, with one top-level folder taking more than two minutes to complete. On-access speeds were pretty fast, while RAM usage was tiny and CPU drain barely noticeable – several of the measures coming in below our baselines taken on unprotected systems. Meanwhile, detection rates were consistently high, with some splendid scores in the RAP sets. With the WildList dealt with satisfactorily, only the clean sets stood between *BitDefender* and another VB100 award. Here, however, things took an unexpected turn, with a handful of PDF files included in a technical design package from leading development house *Corel* flagged as containing JavaScript exploits. These false alarms were enough to deny *BitDefender* an award this month, and did not bode well for the many other products that incorporate the popular engine.

Bkis BKAV Gateway Scan 2910

ItW	100.00%	Polymorphic	64.53%
ItW (o/a)	100.00%	Trojans	35.28%
Worms & bots	62.04%	False positives	0

Once again *Bkis* submitted a selection of products for testing, chasing that elusive first VB100 after some close



On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	1519	90.71%	192	89.73%	14405	79.81%
AhnLab V3	0	100.00%	3606	77.94%	7	99.84%	26573	62.75%
Avast! Free	0	100.00%	360	97.80%	522	93.71%	3160	95.57%
AVG IS	0	100.00%	1269	92.24%	53	97.86%	4279	94.00%
Avira AntiVir	0	100.00%	355	97.83%	0	100.00%	2677	96.25%
BitDefender	0	100.00%	394	97.59%	0	100.00%	3153	95.58%
Bkis Gateway	0	100.00%	6577	59.77%	1601	64.53%	46555	34.74%
Bkis Home	0	100.00%	8736	46.56%	3362	56.10%	46613	34.66%
Bkis Pro	0	100.00%	6204	62.05%	1601	64.53%	46464	34.87%
CA Internet Security Suite Plus	5	99.18%	2226	86.38%	3469	92.58%	21465	69.91%
CA Threat Manager	1	99.84%	3904	76.12%	3469	92.58%	32287	54.74%
Central Command Vexira	0	100.00%	1522	90.69%	192	89.73%	14472	79.71%
Check Point Zone Alarm	0	100.00%	1001	93.88%	0	100.00%	12606	82.33%
Coranti Multicore	7	98.85%	193	98.82%	0	100.00%	951	98.67%
Defenx Security Suite	0	100.00%	2730	83.30%	192	89.73%	15354	78.48%
Digital Defender	1	99.84%	2065	87.37%	192	89.73%	15841	77.80%
eEye Blink	0	100.00%	2845	82.60%	343	82.89%	23229	67.44%
Emsisoft Anti-Malware	0	100.00%	456	97.21%	1371	79.99%	8278	88.40%
eScan ISS	1	99.84%	413	97.47%	0	100.00%	2619	96.33%
ESET NOD32	0	100.00%	870	94.68%	0	100.00%	6690	90.62%
Filseclab Twister	3191	98.48%	2523	84.57%	14085	41.76%	11098	84.44%
Fortinet FortiClient	0	100.00%	2778	83.01%	30	99.36%	28327	60.29%
Frisk F-PROT	0	100.00%	1860	88.62%	0	100.00%	17607	75.32%
F-Secure Client Security	0	100.00%	369	97.74%	0	100.00%	2576	96.39%
F-Secure PSB	0	100.00%	369	97.74%	0	100.00%	2596	96.36%
G DATA	0	100.00%	111	99.32%	0	100.00%	721	98.99%
Ikarus virus.utilities	0	100.00%	212	98.70%	1371	79.99%	6879	90.36%

(Please refer to text for full product names)

calls in recent tests. The first product on test is the *Gateway Scan* version, which came as a 165MB package including all required updates. The installation process is remarkably short and simple, with a single welcome screen before the lightning fast set-up, which even with the required reboot got the system protected less than half a minute after first firing up the installer. The main GUI is unchanged and familiar from previous entries, with a simple layout providing a basic selection of options.

On-demand speeds were fairly sluggish compared to the rest of the field, and the option to scan compressed files

added heavily to the archive scanning time despite only activating scanning one layer deep within nested archives. This time was included in our graphs, in a slight tweak to standard protocol. File access times were very slow as well, and CPU and RAM usage well above average.

In the on-demand scans scores were a little weaker than desirable, with RAP results also fairly disappointing, but the WildList seemed to be handled properly. On-access tests were a little more tricky, with the test system repeatedly suffering a blue screen and needing a restart; this problem was eventually pinned down to a file in the

worms & bots set, which seemed to be causing an error somewhere when scanned. The WildList set was handled smoothly, although initial checking seemed to show several Virut samples not logged; further probing showed that this was down to an issue with the logging sub-system trying to pump out too much information too quickly, and retrying brought together a full set of data showing complete coverage. On its third attempt, *Bkis* becomes this month's first new member of the elite circle of VB100 award holders.

Bkis BKAV Home Edition 2910

ItW	100.00%	Polymorphic	56.10%
ItW (o/a)	100.00%	Trojans	35.28%
Worms & bots	62.05%	False positives	0

The home version of *BKAV* resembles the *Gateway Scan* solution in many respects, with another 250MB installer and

a similarly rapid and simple set-up process. The interface is also difficult to tell apart, except for the colour scheme which seemed to be a slightly different shade of orange from the *Gateway* product.

Also similar were the slowish speeds both on demand and on access, with pretty heavy resource consumption. The problem with the on-access tests of the worms & bots set also recurred, although in this case we only observed the product crashing out rather than the whole system going down. Once again, logging issues were noted on-access, which were easily resolved by performing multiple runs. The logging system was added by the developers to fit in with our requirements, and real-world users would simply rely on the default auto-clean system. Scores were found to be generally close to those of the *Gateway* product, although with slightly poorer coverage of older and more obscure polymorphic viruses; the WildList and clean sets were handled very nicely, and a second VB100 is earned by *Bkis*.

Bkis BKAV Pro 2910

ItW	100.00%	Polymorphic	64.53%
ItW (o/a)	100.00%	Trojans	35.28%
Worms & bots	62.05%	False positives	0

The third of this month's entries from *Bkis* is a 'professional' edition, but once again few differences were

discernable in

the install package or set-up process, the interface design, layout or the performance.

Scores – when put together avoiding problems with the logs – showed similar if not identical rates to the *Gateway* solution, and with an identical showing in the core certification sets *Bkis* makes it a clean sweep, earning a hat-trick of VB100 awards in a single go – surely some kind of record.

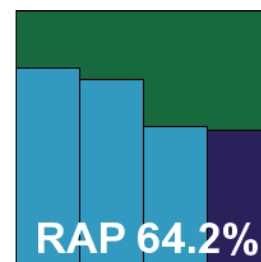
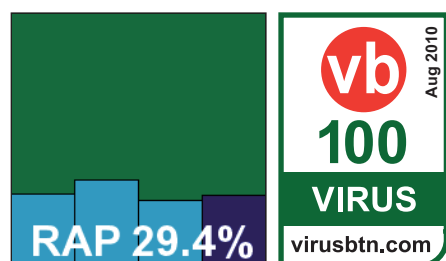
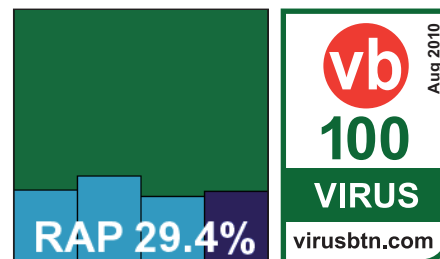
CA Internet Security Suite Plus 6.0.0.285

ItW	99.18%	Polymorphic	92.58%
ItW (o/a)	99.18%	Trojans	69.87%
Worms & bots	86.38%	False positives	0

CA's home-user product was provided as a 157MB installer package needing further online updates; the initial set-up process was fairly straightforward, with a handful of standard steps including a EULA, plus an optional 'Advanced' section offering options on which components to install. After

a reboot, a quick check showed it had yet to update, so this was initiated manually. There were a few moments of confusion between two sections of the slick and futuristic interface – one, labelled 'Update settings', turned out to provide settings to be updated, while another, in a section marked 'Settings' and labelled 'Update options', provided the required controls for the updates. The update itself took a little over half an hour, at the end of which a second update was required.

The interface has a rather unusual look and feel and is at first a little tricky to navigate, but with some familiarity – mostly gained by playing with the spinning-around animated main screen – it soon becomes reasonably usable. With some sensible defaults, and a few basic options provided too, zipping through the tests proved fairly pleasant, with some remarkable speed improvements in the 'warm' scans on demand and a reasonable footprint on



On-access tests contd.	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
K7 Total Security	0	100.00%	1225	92.51%	0	100.00%	12496	82.48%
Kaspersky Anti-Virus 6.0	0	100.00%	587	96.41%	0	100.00%	5240	92.66%
Kaspersky IS 2011	0	100.00%	711	95.65%	0	100.00%	9178	87.14%
Keniu Antivirus	0	100.00%	568	96.53%	0	100.00%	6297	91.17%
Kingsoft IS Advanced	8	99.999%	8666	46.99%	4828	58.88%	61082	14.38%
Kingsoft IS Standard	8	99.999%	9174	43.88%	4828	58.88%	63435	11.08%
Lavasoftware Ad-Aware Professional	0	100.00%	572	96.50%	1054	73.53%	4384	93.85%
Lavasoftware Ad-Aware Total Security	0	100.00%	111	99.32%	0	100.00%	733	98.97%
McAfee Total Protection	5	99.9997%	1012	93.81%	1	99.999%	9754	86.33%
McAfee VirusScan	5	99.9997%	1290	92.11%	1	99.999%	14157	80.16%
Microsoft Security Essentials	0	100.00%	688	95.79%	0	100.00%	5720	91.98%
Nifty Security24	0	100.00%	687	95.80%	0	100.00%	8703	87.80%
Norman Security Suite	0	100.00%	2845	82.60%	343	82.89%	23230	67.44%
PC Tools IS	0	100.00%	1865	88.59%	0	100.00%	14549	79.61%
PC Tools Spyware Doctor	0	100.00%	1865	88.59%	0	100.00%	14445	79.75%
Preventon Antivirus	1	99.84%	2065	87.37%	192	89.73%	15841	77.80%
Proland Protector Plus	0	100.00%	1434	91.23%	192	89.73%	13737	80.74%
Qihoo 360	0	100.00%	433	97.35%	0	100.00%	2790	96.09%
Quick Heal AntiVirus	0	100.00%	4505	72.44%	43	96.86%	30659	57.03%
Returnil RVS	0	100.00%	1911	88.31%	0	100.00%	17413	75.59%
Rising IS	0	100.00%	7216	55.86%	3576	70.87%	36444	48.92%
Sophos Endpoint	0	100.00%	602	96.32%	0	100.00%	6295	91.18%
SPAMfighter VIRUSfighter	1	99.84%	2063	87.38%	192	89.73%	15776	77.89%
Sunbelt VIPRE	0	100.00%	355	97.83%	1054	73.53%	6186	91.33%
Symantec Endpoint Security	0	100.00%	2036	87.55%	0	100.00%	15827	77.82%
Trustport AntiVirus	0	100.00%	161	99.02%	0	100.00%	1015	98.58%
VirusBuster Professional	0	100.00%	1522	90.69%	192	89.73%	14462	79.73%

(Please refer to text for full product names)

access. RAM usage while the system was idle was notably high, hinting at some activity going on when nothing else requires resources, but this effect was much less noticeable when the system was busy.

Detection tests brought up no major issues until an attempt to display the results of one particularly lengthy scan caused the GUI to grey out and refuse to respond – not entirely unreasonable, given the unlikelihood of any real-world user

experiencing such large numbers of infections on a single system. Re-running scans in smaller chunks easily yielded results, which proved no more than reasonable across the sets.

In the clean sets, a single item from *Sun Microsystems* was flagged as potential adware, which is perhaps permissible under the VB100 rules, but in the WildList set a handful of items added to the most recent list were not detected, either

on demand or on access, and CA's home suite does not make the grade for a VB100 award this month.

CA Threat Manager 8.1.660.0

ItW	99.84%	Polymorphic	92.58%
ItW (o/a)	99.84%	Trojans	54.84%
Worms & bots	76.20%	False positives	0

The business-oriented offering from CA is considerably less funky and modern than its home-user sibling, having remained more or less identical since as long ago as 2006. The installer – which we have kept on file for several years – is in an archive of a complete installation

CD which covers numerous other components including management utilities and thus measures several hundred MB. It runs through fairly quickly now with the benefit of much practice, but includes a number of stages including several different EULAs to scroll through. A reboot is needed to complete.

Once set up and ready, the interface is displayed by the browser and suffers a little from some suspect design decisions, with many of the options ephemeral and subject to frequent resetting. Buttons and tabs can be slow to respond, and the logging system is both awkward to navigate and easily overwhelmed by large amounts of information. However, scanning speeds are as impressive as ever, with low drain on resources and minimal slowdown on accessing files. Behaviour was generally good throughout, with no problems with stability or loss of connection to the controls. Detection results were somewhat poorer than the home-user product in some sets, however, and with a single WildList file missed CA fails to earn any VB100 awards this month.

Central Command Vexira 6.2.54

ItW	100.00%	Polymorphic	89.73%
ItW (o/a)	100.00%	Trojans	82.94%
Worms & bots	92.09%	False positives	0

Vexira was provided this month as a 55MB installer accompanied by a 66MB update bundle. The set-up process seemed to run through quite a number of steps but they were all fairly standard and didn't require much thought to get through; with no reboot needed, protection was in place in under a minute. On firing up the interface, we recoiled slightly from the fiery red colour scheme, glowing brightly against the glittery Vista desktop, but its design and layout is

familiar from the VirusBuster product on which it is closely modelled and we soon found ample and fairly accessible controls. Set-up

of on-demand scans is perhaps a little fiddly, but after some practice the process soon became second nature.

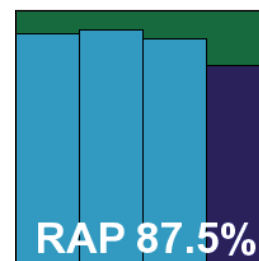
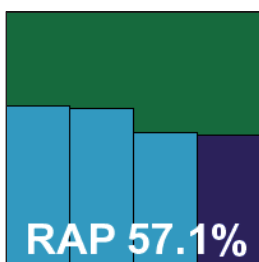
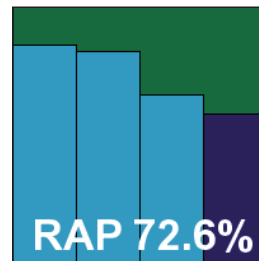
Scanning speeds were pretty decent, especially in the archive set, with most archive types being scanned to some depth by default, although the new zipx format seemed to be ignored. On-access speeds were average overall, and rather slow in some types of files, but resource usage was generally fairly low. Detection rates were fairly decent across the sets, with a reasonable showing in the RAP sets, and with no problems in the WildList or clean sets Vexira makes it safely to another VB100 pass.

Check Point Zone Alarm Security Suite 9.1.57.000

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	91.26%
Worms & bots	95.53%	False positives	0

Check Point submitted its mid-range suite for this test, which was provided as a 133MB installer with an additional 68MB of

updates in a fairly raw state for simply dropping into place. The installation process went through several steps, including the standard EULA and warnings about clashing with other products, as well as the offer of a browser toolbar and some set-up for the 'auto-learn' mode. On completion a reboot is required and a quick scan is run without asking the user. The design and layout are sober, serious and fairly easy to find one's way around, and ample controls were provided, rendering testing fairly easy. Scanning speeds were excellent with the default settings – which are fairly light – and still fairly decent with deeper and more thorough scanning enabled. Resource consumption was not too high, and file access times not bad either.



Archive type handling		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
AhnLab V3	OD	X	√	X/√	X/√	X	√	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Avast Free	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
AVG IS	OD	√	√	√	√	√	√	√	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	X/8	X/8	X/√	X/√	X/√	X/8	1/√	1/√	√
Bkis Gateway	OD	X	X	X/1	X/1	X/1	X	X/1	X/1	X/1	X/1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bkis Home	OD	X	X	X/1	X/1	X/1	X	X/1	X/1	X/1	X/1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bkis Pro	OD	X	X	X/1	X/1	X/1	X	X/1	X/1	X/1	X/1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
CA ISS Plus	OD	X	√	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	1	X	X	X	1	X	√
CA Threat Manager	OD	X	√	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	1	X	X	X	1	X	√
Central Command Vexira	OD	2	√	√	√	X	X	√	√	√	X	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Check Point Zone Alarm	OD	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Coranti Multicore	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/1	X	X	X	X/√	X	X	X	X/1	X/1	X/√
Defenx Security Suite	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Digital Defender	OD	1	1	1	1	1	X	1	X	1	1	√
	OA	1	1	X	X	X	X	1	X	1	X	√
eEye Blink	OD	X	4/√	3/√	1	4/√	4/√	4/√	4/√	2/√	1	√
	OA	X	X/√	X/√	X	X/√	X/√	X/√	X/√	X/√	X/1	√
Emsisoft Anti-Malware	OD	2	2	2	2	2	2	2	1	2	2	√
	OA	2	2	2	2	2	2	2	1	2	2	√

Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels. (Please refer to text for full product names)

In the detection sets we encountered a single issue where a scan seemed to hang. When trying to reboot the system to recover from this, another hang occurred at the logout screen, and the machine needed a hard restart. The problem did not recur though, and results were soon obtained, showing the usual excellent detection rates across the sets, with a pretty decent showing in the RAP sets. With no issues in the WildList or clean sets, *Check Point* comfortably regains its VB100 certified status.

Coranti 2010 1.000.00042

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	98.85%	Trojans	99.47%
Worms & bots	99.50%	False positives	15

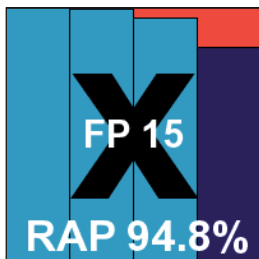
Coranti's multi-engine approach makes for a fairly hefty set-up/install process, with an initial installer weighing in at 45MB replaced with a whole new one of similar bulk as soon as it was run. With that done, online updating was required, and with an additional 270MB of data to pull down this took quite a lot longer to complete. Once this had finished, the actual install process was fairly fast and simple, but did require a reboot at the end.

Once up and running, we found the main interface reassuringly complete and serious-looking, with a thorough set of controls for the most demanding of users well laid out and simple to operate. Scanning speeds were rather slow, as might be expected from a solution that combines three separate engines, with long delays to access files, but usage of RAM and CPU cycles was lighter than expected.

The multi-engine technique pays off in the detection rates of course, with some scorching scores across the test sets, and the RAP sets particularly thoroughly demolished. The flip side is the risk of false positives, and this proved to be *Coranti's* Achilles' heel this month, with that handful of PDFs from *Corel* flagged by one of the engines as containing JavaScript exploits, thus denying the firm a VB100 award. This was made doubly sure by the fact that certain file extensions commonly used by spreading malware were not analysed on access.

Defenx Security Suite 2010 3063.454.0728

ItW	100.00%	Polymorphic	89.73%
ItW (o/a)	100.00%	Trojans	83.00%
Worms & bots	91.94%	False positives	0



Defenx is based in Switzerland and provides a range of tools tuned for the needs of the company's local markets.

The Security

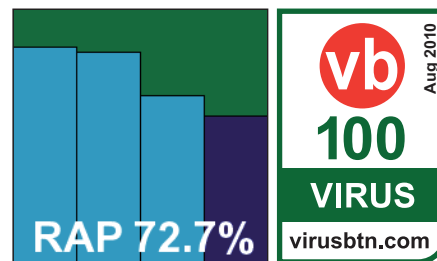
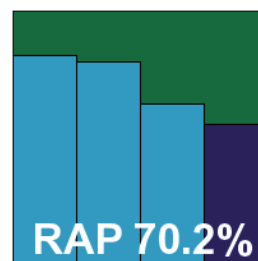
Suite is an adaptation of *Agnitum's Outpost*, combining the Russian company's well-regarded firewall technology with anti-malware centred around the *VirusBuster* engine. Despite the multiple functions, the installer is a reasonably lightweight 92MB with all updates included, but as might be expected it goes through a number of stages in the set-up process, many of which are associated with the firewall components. Nevertheless, with some quick choices the full process is completed in under a minute, and no reboot is required.

Controls are clearly labelled and easy to use, and tests ran through swiftly, aided by some nifty improvement in scanning times after initial familiarization with files. On-access speeds were not outstanding at first but also improved greatly, and resource consumption was fairly low. Detection rates in the main sets were decent, with the scan of the clean set producing a number of warnings of packed files but no more serious alerts; the WildList was handled without problems, and a VB100 is duly earned by *Defenx*.

Digital Defender AntiVirus 2.0.43

ItW	99.84%	Polymorphic	89.73%
ItW (o/a)	99.84%	Trojans	80.71%
Worms & bots	88.44%	False positives	0

Making its third consecutive appearance on the VB100 test bench, *Digital Defender's* 47MB installer runs through the standard series of steps and needs no reboot to complete, the whole business taking just a few moments. The interface is clean and clear, providing an impressive degree of control for what appears on the surface to be a pared-down product. The product ran just as cleanly, causing no upsets through the tests and recording some respectable scanning speeds with a solid regularity but no indication of smart filtering of



Archive type handling contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
eScan ISS	OD	9	5	4	3	5	5	5	4	5	8	√
	OA	X/√	X/√	X/8	X/8	X/√	X/√	X/√	X/8	X/√	X/√	√
ESET NOD32	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Filseclab Twister	OD	X/√	X/√	X/√	X/√	X/√	X/√	1/√	X	2/√	X	X/√
	OA	X	X	X	1	X	X	1	X	X	X	X
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	4	1	√
	OA	X	√	√	√	√	√	√	√	4	1	√
Frisk F-PROT	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	2	X	X	X	X	2	2	√
F-Secure Client Security	OD	X/√	√	√	√	√	√	√	8	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure PSB	OD	X	√	√	√	√	√	√	2	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
G DATA	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	3/√	4/√	√	√	√	8/√	√	√	√
Ikarus virus.utilities	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	2	1	1	1	1	1	1	1	1	1	√
K7 Total Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	1	1	X	X	X	1	1	√
Kaspersky Anti-Virus 6.0	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kaspersky IS 2011	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Keniu Antivirus	OD	√	√	X	X	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Kingsoft IS Advanced	OD	X	√	√	1	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kingsoft IS Standard	OD	X	√	√	X	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Lavasoft Ad-Aware Professional	OD	X	X	√	√	X	X	1	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	X
Lavasoft Ad-Aware Total Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	3	4	√	√	√	8	8	√	√
McAfee Total Protection	OD	2	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√

Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels. (Please refer to text for full product names)

previously scanned items. File access lags were fairly low, and RAM usage notably minimal.

Detection rates were fairly decent in general, with no problems in the clean set, but in the WildList set a single sample of a W32/Ircbot variant was not detected, which came as a surprise, given the clean sheets of other products based on the same (*VirusBuster*) technology. *Digital Defender* thus misses out on a VB100 award this month.

eEye Digital Security Blink 4.6.6

ItW	100.00%	Polymorphic	84.55%
ItW (o/a)	100.00%	Trojans	70.02%
Worms & bots	85.34%	False positives	1

Blink has long been a popular entrant in our comparatives, with its clean, neat design and interesting extras – notably the vulnerability monitoring which is its major selling point. The installation process has a few extras in addition to the standard steps, including the option to password-protect the

product settings, which is ‘highly recommended’ by the developers for added security. An initial configuration wizard follows the install, with no reboot needed, which sets up the additional components such as a firewall (disabled by default), HIPS and ‘system protection’ features, many of which are not covered by our tests. The interface, like the set-up process, is displayed in a pleasant pastelly peach tone, and as usual we found it slick, smooth and clearly laid out.

Running through the speed tests proved rather a test of endurance, with the sandbox facility adding some serious time onto the on-demand scans – not so much ‘blink and you’ll miss it’ as ‘take forty winks while you wait for it to finish’. On-access times were just as sluggish, although RAM usage was no higher than many other entrants this month. In the infected sets detection rates were generally pretty decent. In the WildList set all was well, after some problems with W32/Virut in recent comparatives, but luck was not on *eEye*’s side, with a single sample in the clean set – part of a DVD authoring suite from major developer *Roxio* – labelled as a Swizzor trojan, and once again *Blink* is denied a VB100 despite a generally decent showing.

Emsisoft Anti-Malware 5.0..060

ItW	100.00%	Polymorphic	79.99%
ItW (o/a)	100.00%	Trojans	92.25%
Worms & bots	98.79%	False positives	0

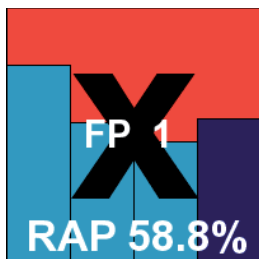
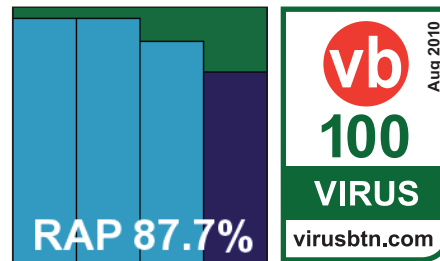
Having rebranded itself slightly to drop its former ‘A-Squared’ name in favour of a more directly relevant title,

Emsisoft’s

product has grown in slickness and clarity from test to test. The product was provided as a 103MB installer package, which we updated and activated online prior to commencing testing, although a fully updated package of roughly the same size was also provided later. The initial phase of the set-up followed the standard path, but some post-install set-up included activation options ranging from a completely free trial, via a longer trial process requiring submission of contact information, to fully paid licensing. An impressive range of languages were also offered. On completing installation, with no need for a reboot, the product offered to ‘clean your computer’, by which it meant perform a scan. On looking over the installed items, we noted the old ‘a2’ references still lurking in some paths, as is common in the early stages of a rebranding.

Initial testing was somewhat hampered by odd responses to our testing tools; some tweaking of settings made the product operate more in line with our needs, but it still disrupted the gathering of performance data, and we had to disable the behaviour blocker to get our scripts to run successfully. At one point during the simple opening of clean files and snapshotting of system performance information, the whole system locked up badly and had to be restarted using the power reset button. Eventually, however, we got some results which showed some very heavy on-access overheads on first visit. Scanning speeds increased massively in the ‘warm’ scans, and very little RAM but a lot of CPU cycles were used. On-demand speeds were fairly sedate in some sets, but reasonable in others, notably the media & documents set.

In the infected sets, scores were truly splendid across the board. The clean sets yielded a couple of alerts, one noting that the popular IRC tool *MIRC* is indeed an IRC tool, and the other pointing out that a tool for converting PDFs to Word documents – recommended by the editors of a popular download site in recent months – could be labelled a ‘PDF cracker’ and thus qualified as riskware. Both these alerts were comfortably allowed as only ‘suspicious’ under the VB100 rules, and *Emsisoft* only required a clean run through the WildList set to qualify for its first VB100 award. After an initial scare when some items appeared not to be spotted, rechecking of logs showed full coverage,



Archive type handling contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
McAfee VirusScan	OD	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X	√
Microsoft Security Essentials	OD	√	√	√	√	2	2	2	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Nifty Security24	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Norman Security Suite	OD	X	√	√	1	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
PC Tools IS	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	X
PC Tools Spyware Doctor	OD	2	√	√	√	√	√	√	√	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	X
Preventon Antivirus	OD	1	1	1	1	1	X	1	X	1	X	√
	OA	1	1	1	1	1	X	1	X	1	X	X/√
Proland Protector Plus	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Qihoo 360	OD	√	√	8	8	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Quick Heal AntiVirus	OD	X/2	X/5	X	X	2/5	X	2/5	X/1	2/5	X	X/√
	OA	2	X	X	X	1	X	X	X	1	X	√
Returnil RVS	OD	5	5	5	5	5	√	5	5	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Rising IS	OD	X	X	9	9	9	9	9	√	9	9	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Sophos Endpoint	OD	X	X/5	X/5	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/5	X/5	X/√
SPAMfighter VIRUSfighter	OD	1	1	1	1	1	X	1	X	1	X	√
	OA	X/1	X/1	X	X	X	X	X/1	X	X/1	X	X/√
Sunbelt VIPRE	OD	X	X	√	√	X/√	X	X/√	X	X/√	X/1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Symantec Endpoint Security	OD	3/√	3/√	3/√	3/√	3/√	3/√	3/√	1/5	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Trustport Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	X/√
VirusBuster Professional	OD	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√

Key: X - Archive not scanned; X/√ - Default settings/thorough settings; √ - Archives scanned to depth of 10 or more levels; [1-9] - Archives scanned to limited depth; EXT* - Eicar test file with random extension; All others - detection of Eicar test file embedded in archive nested up to 10 levels. (Please refer to text for full product names)

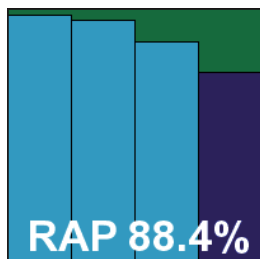
and Emsisoft's product joins the ranks of VB100 certified solutions, with our congratulations.

eScan Internet Security Suite 11.0.1111.735

ItW	99.84%	Polymorphic	100.00%
ItW (o/a)	99.84%	Trojans	97.35%
Worms & bots	98.36%	False positives	0

The latest offering from VB100 regular *eScan* has a pretty nifty set-up process from its sizeable 127MB install package, which is slowed down by the installation of some additional libraries, and includes a quick scan of vital areas during the process. Once up and running, the main interface is a delight to behold, with a series of icons along the bottom which enlarge when rolled over like the task panel on a *Mac*. This encouraged much playing among the lab team.

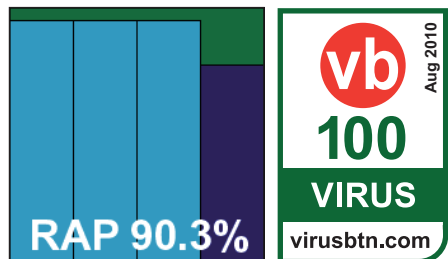
Having tired of this little pleasure, testing proceeded apace, helped by the ample configuration controls provided beneath the silky smooth front end. On-demand speeds were rather on the slow side, speeding up greatly on second viewing of known files, and on-access lags also seemed to benefit from familiarity, while RAM usage was surprisingly low. Detection rates, meanwhile, were very decent, with nothing to complain about in any of the main or RAP sets. The clean set scan included a few alerts on files marked as 'Null:Corrupted', which was no problem, but in the WildList set a single sample of W32/Koobface was missed, thus denying *eScan* a VB100 award this month.



ESET NOD32 Antivirus 4.2.40.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	94.44%
Worms & bots	98.75%	False positives	0

ESET provided its current product, with all updates rolled in, as a very compact 40MB package. Installing ran as per usual, with information and options presented regarding taking part in



the ThreatSense.net intelligence system, and the company's trademark insistence on a decision regarding the detection of 'potentially unwanted' items. No reboot was needed to finish off, and the whole job was done in a minute or so.

Once installed, the familiar and much admired interface provided a great abundance of fine-tuning options in its many advanced set-up pages, with a good balance between simplicity on the surface and more technical completeness beneath. Once again, however, we noted that, despite what appeared to be options to enable it, we were unable to persuade the product to unpack archive files on access.

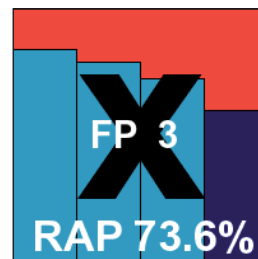
Generally, the product ran through the tests pretty solidly, but we did observe a few minor issues with the interface, with a number of scans reaching 99% and remaining there without ever reaching the end. A check of the logs showed that the scans had actually finished but hadn't quite managed to display this fact properly. Also, in the most stressful portions of the on-access tests we saw some messages warning that the scanner had stopped working, but it appeared to be still running OK and no gap in protection was discernable.

Scanning speeds were pretty decent, especially given the thorough defaults on demand, and there were some reasonable and reassuringly stable file access times. Memory usage was among the lowest in this month's comparative, with CPU drain not breaking the bank either. Detection rates were as excellent as ever, with some superb RAP scores; no issues emerged in the WildList or clean sets, and *ESET* continues its monster unbroken run of VB100 passes.

Filseclab Twister V7 R3 (version 7.3.4.9985)

ItW	98.48%	Polymorphic	41.76%
ItW (o/a)	98.48%	Trojans	86.23%
Worms & bots	85.99%	False positives	3

Twister has become a fairly familiar face in our comparatives, edging ever closer to that precious first VB100 award. The installer, 52MB with 26MB of updates, runs through quickly and easily with no surprises, ending with a call for a reboot. The interface is slick and serious-looking, with lots of controls, buttons, options and dialogs, but remains fairly simple to navigate after a little initial exploration.



Scanning speeds and on-access overheads were a bit of a mixed bag, with some fast times and some slower ones,

On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	1.67	22.06	1.67	21.72	230.72	21.72	8.89	27.74	8.89	8.82	297.03	23.69
AhnLab V3	3.01	2.94	2.05	37.83	37.04	5.52	15.71	15.92	15.92	14.14	39.79	24.32
Avast! Free	396.04	437.73	13.66	91.98	90.22	73.30	46.80	52.12	43.27	64.49	189.02	95.60
AVG IS	0.67	332.67	0.67	17.18	27.76	17.18	5.78	5.85	5.49	5.52	15.01	11.32
Avira AntiVir	7.47	7.46	7.47	73.30	74.46	73.30	30.57	31.56	30.57	27.15	74.93	72.95
BitDefender	19.66	21.38	19.66	23.81	23.89	23.81	286.64	362.07	286.64	6.14	16.80	16.50
Bkis Gateway	89.43	91.39	0.63	3.71	4.12	3.68	4.55	4.53	3.75	3.29	9.06	7.66
Bkis Home	89.43	91.39	0.88	4.14	4.16	4.04	4.51	4.58	3.91	3.56	8.92	7.97
Bkis Pro	89.43	93.45	0.86	4.13	4.10	4.07	4.62	4.55	2.69	3.46	9.05	9.03
CA ISS Plus	2.12	2079.20	2.12	39.76	740.72	39.76	24.14	143.32	24.14	13.06	297.03	35.09
CA Threat Manager	3.34	3.29	3.34	49.91	49.91	49.91	37.59	33.89	37.59	18.43	44.24	49.50
Central Command Vexira	10.91	11.06	3.37	31.48	31.91	29.14	23.16	23.97	17.78	10.42	28.29	22.18
Check Point Zone Alarm	308.03	286.79	2.56	27.43	118.27	23.69	60.35	63.11	13.33	257.97	1386.14	22.36
Coranti Multicore	2.71	2.71	2.71	6.73	6.76	6.73	3.96	3.99	3.96	3.18	8.50	8.53
Defenx Security Suite	1.69	21.27	1.69	17.77	223.39	17.77	9.25	28.78	9.25	4.16	231.02	11.18
Digital Defender	4.79	4.83	4.79	15.53	15.57	15.53	18.80	18.90	18.80	10.53	28.39	28.29
eEye Blink	1.43	1.43	1.34	2.02	2.02	2.02	0.87	0.86	0.87	0.62	0.62	0.62
Emsisoft Anti-Malware	6.13	7.01	6.13	9.88	9.81	9.88	17.91	13.45	17.91	12.00	32.24	32.24
eScan ISS	10.46	286.79	10.46	4.21	13.72	4.21	3.25	36.59	3.25	2.61	90.40	7.02
ESET NOD32	4.06	4.12	4.06	57.92	58.64	57.92	14.89	15.02	14.89	15.40	41.58	41.38
Filseclab Twister	41.38	41.38	0.97	43.84	43.71	13.10	7.45	6.18	6.16	3.79	9.63	9.66
Fortinet FortiClient	6.52	6.60	6.52	8.47	8.71	8.47	6.27	6.23	6.27	11.34	30.46	30.46
Frisk F-PROT	9.83	9.84	9.83	17.70	17.95	17.70	48.79	43.54	48.79	36.85	87.55	99.01
F-Secure Client Security	10.66	10.62	1.99	26.50	26.65	23.93	18.95	18.15	14.61	93.81	231.02	22.54
F-Secure PSB	10.42	10.38	10.42	23.22	24.31	23.22	17.78	17.50	17.78	79.38	231.02	213.25
G DATA	4.02	2772.27	4.02	28.78	740.72	28.78	15.29	116.60	15.29	14.33	244.61	38.50
Ikarus virus.utilities	29.81	29.39	29.18	18.62	18.82	18.62	23.89	23.01	23.89	10.98	29.81	29.49

(Please refer to text for full product names)

depending on file types. Meanwhile, performance measures showed some very high memory consumption but not too much pressure on the CPU.

On-access scanning does not offer the option simply to block access to infected files, and logging seems only to function once files have been 'cleaned' – so we had to let the product romp through our sets, destroying as it went,

which took quite some time. On-demand scans were much easier and more cooperative, and in the end some pretty decent scores were noted across the sets, with a solid showing in the RAP sets, declining slowly through the reactive weeks but with a steepish drop into week +1.

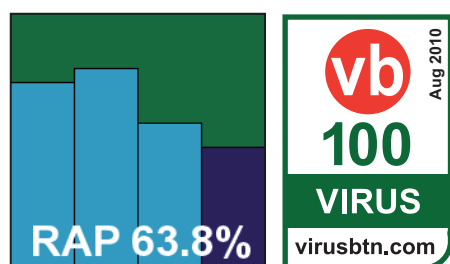
A couple of false alarms were produced in the clean sets, with the popular VLC video client being labelled as a TDSS

trojan. The WildList set highlighted some problems with the complex Virut polymorphic samples, with a fair number missed, alongside a handful of the static worms and bots in the set. For now, that first VB100 award remains just out of reach for *Filseclab*.

Fortinet FortiClient Endpoint Security 4.1.3.143

ItW	100.00%	Polymorphic	99.36%
ItW (o/a)	100.00%	Trojans	60.30%
Worms & bots	83.01%	False positives	0

Fortinet's product came as a slender 9.8MB main package with an additional 150MB of updates. The set-up process was



fairly routine, enlivened by noticing the full 'endpoint security' nomenclature (not mentioned elsewhere in the main product), and once again the option to install the full paid product or a free edition. Not having been provided with activation codes, we went for the free version, which seemed to meet our needs adequately. The set-up process had fairly few steps to go through and didn't require a reboot to complete.

The product's interface has remained pretty much unchanged for some time, and we have always found it fairly clearly laid out and intuitive. In the performance tests some fairly sluggish scanning times were not improved by faster 'warm' performances. Access lag times were pretty hefty, while use of system resources was on the heavy side too. Scans of infected sets proved even slower: a series of scheduled jobs set to run over a weekend overlapped each other despite what we assumed would be large amounts of extra time given to each scan. Returning after the weekend we found two of the scans still running, which eventually finished a day or two later. Another oddity observed was that the update package provided seemed to disable detection of the Eicar test file, which is used in our measures of depth of archive scanning. The sample file was detected with the original definitions in the base product however, so the data on compressed files was gathered prior to updating.

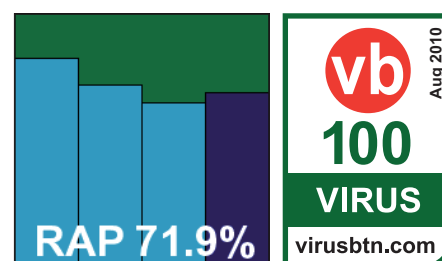
In the end we obtained a full set of data, showing some fairly respectable scores in most sets, with a good start to the RAP sets declining sharply in the more recent weeks.

The WildList and clean sets presented no problems for the product, and a VB100 award is duly granted.

Frisk F-PROT Antivirus for Windows 6.0.9.3

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	78.30%
Worms & bots	89.38%	False positives	0

Frisk's installer comes as a 25MB package, with an extra 48MB of updates. In offline situations these are applied simply by



dropping the file into place after the installation process – which is fast and simple – and prior to the required reboot. Once the machine was back up after the reboot we quickly observed that the product remains the same icy white, pared-down minimalist thing it has long been.

The basic set of configuration options simplified testing somewhat, and with reasonable speeds in the scanning tests (impressively fast in the archive sets given the thorough defaults), lag times also around the middle of the field, and fairly low use of RAM but average CPU drain when busy, we quickly got to the end without problems. As in many previous tests, error messages were presented during lengthy scans of infected items warning that the program had encountered an error, but this didn't seem to affect either scanning or protection.

Detection rates were pretty decent across the sets, with just a single suspicious alert in the clean sets and no problems in the WildList; *Frisk* thus earns another VB100 award.

F-Secure Client Security 9.01 build 122

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.43%
Worms & bots	98.67%	False positives	0

F-Secure once again submitted two fairly similar products to this test. The first, *Client Security*, came as a 58MB installer with an additional updater measuring a little under 100MB. Installation was a fairly unremarkable process, following the standard path of welcome, EULA, install location, and going on to offer centralized or local install methods – implying that this is intended as a business product for installing in large networks. It all completed

On-demand throughput (MB/s) contd.	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	De-fault (cold)	Default (warm)	All files	De-fault (cold)	Default (warm)	All files
K7 Total Security	9.87	9.89	9.87	14.57	14.57	14.57	32.30	37.59	32.30	7.07	19.08	18.99
Kaspersky AV 6.0	6.34	2772.27	6.34	55.85	2345.61	55.85	26.36	382.19	26.36	16.92	756.07	45.45
Kaspersky IS 2011	5.15	756.07	5.15	173.75	287.22	173.75	163.79	167.79	163.79	171.98	519.80	462.05
Keniu Antivirus 1.0	2.14	489.22	2.14	16.69	42.65	16.69	7.72	26.87	7.72	6.03	40.97	16.21
Kingsoft IS Advanced	2.32	2.33	2.32	38.45	38.45	38.45	9.10	9.09	9.10	21.95	59.83	58.98
Kingsoft IS Standard	2.32	2.33	2.32	40.44	40.21	40.44	9.14	9.15	9.14	19.11	60.27	51.34
Lavasoft Ad-Aware Pro	86.63	86.63	NA	15.28	15.41	15.28	2.53	2.27	2.53	2.81	7.51	7.55
Lavasoft Ad-Aware TS	4.11	2772.27	4.11	22.34	879.60	22.34	13.57	105.84	13.57	7.48	101.42	20.09
McAfee TP	2.38	3.50	2.38	20.40	108.26	20.40	12.53	70.20	12.53	6.33	44.24	17.01
McAfee VirusScan	132.01	129.95	2.75	19.63	19.82	18.04	11.19	11.22	11.02	7.59	20.38	20.09
MS Security Essentials	3.85	3.83	3.85	18.84	18.97	18.84	25.77	26.77	25.77	9.64	26.57	25.91
Nifty Security24	3.03	1386.14	3.03	26.65	351.84	26.65	11.08	61.98	11.08	6.22	132.01	16.70
Norman Security Suite	1.06	1.06	1.06	3.10	3.10	3.10	5.81	5.73	5.81	3.97	10.56	10.66
PC Tools IS	3.02	3.16	3.02	60.14	69.67	60.14	11.76	11.90	11.76	7.53	20.24	20.24
PC Tools SD	3.49	3.63	0.96	72.17	73.30	14.48	12.96	13.00	12.88	11.22	30.13	30.13
Preventon Antivirus	4.66	4.65	4.66	15.80	15.87	15.80	19.11	18.69	19.11	16.12	42.87	43.32
Proland Protector Plus	8.13	8.14	8.13	28.96	29.02	28.96	7.93	7.94	7.93	5.49	14.44	14.75
Qihoo 360	3.00	2.98	3.00	22.13	22.02	22.13	12.67	12.60	12.67	7.53	20.09	20.24
Quick Heal AntiVirus	3.18	3.13	2.07	60.92	60.40	58.64	11.94	11.86	11.76	12.14	32.49	28.58
Returnil RVS	7.02	7.35	7.02	15.04	15.23	15.04	8.65	8.77	8.65	13.76	38.68	36.96
Rising IS	1.90	1.97	1.90	11.04	11.82	11.04	5.57	5.94	5.57	5.80	18.04	15.57
Sophos Endpoint	173.27	277.23	2.61	15.23	15.53	15.23	21.43	20.47	17.24	7.88	19.80	16.21
SPAMfighter VIRUSfighter	4.49	4.44	NA	15.13	15.26	15.13	15.60	17.55	15.60	8.97	21.00	24.11
Sunbelt VIPRE	154.02	154.02	2.85	25.22	25.04	24.82	2.38	2.37	2.38	2.80	7.21	7.43
Symantec ES	3.77	3.77	3.46	32.13	31.56	30.46	17.91	18.06	17.78	14.95	43.32	40.18
Trustport AntiVirus	2.34	2.36	2.34	13.40	16.12	13.40	8.99	9.06	8.99	4.47	12.36	12.00
VirusBuster Pro	10.75	10.79	3.35	31.27	31.00	28.26	22.48	22.78	17.11	18.76	51.66	42.65

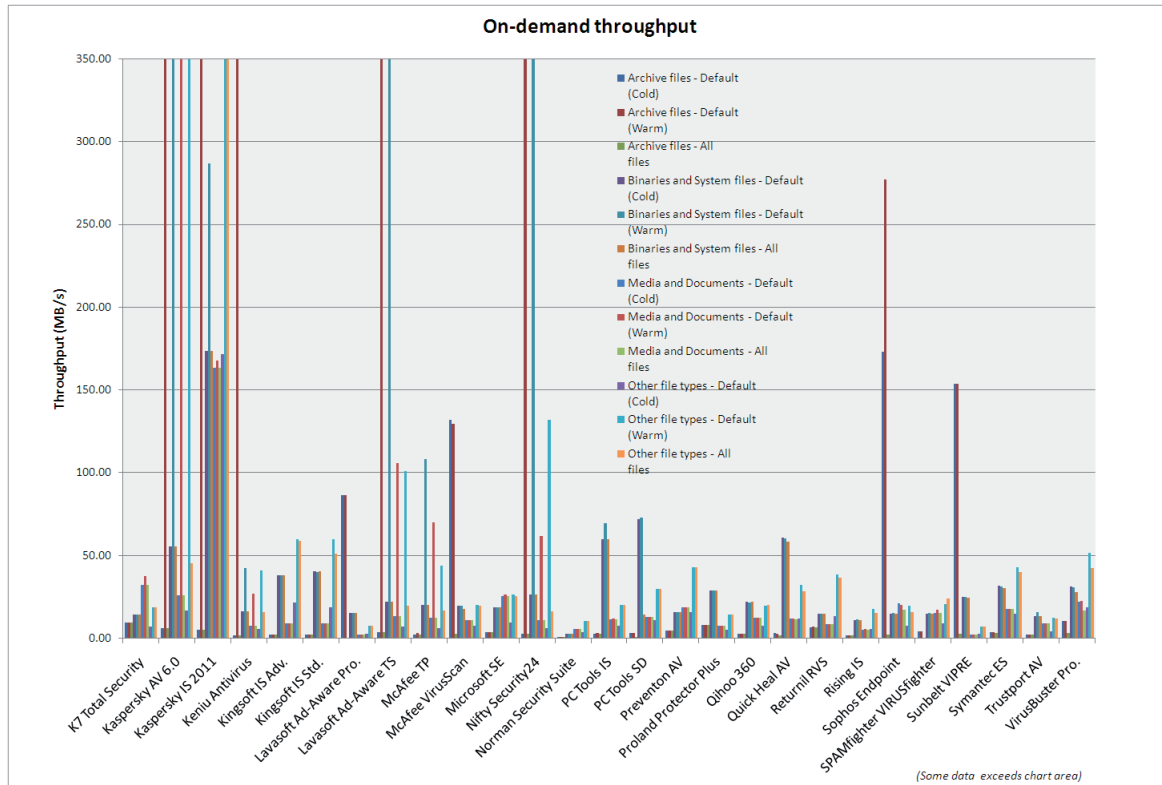
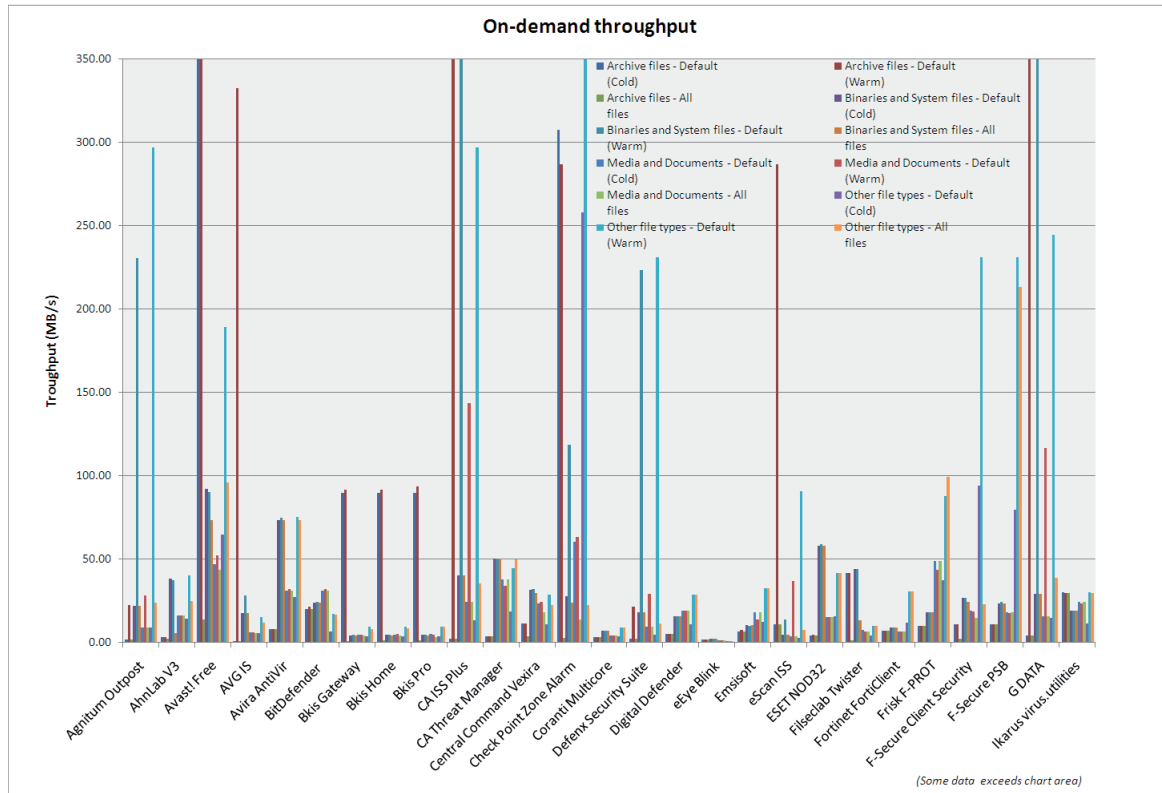
(Please refer to text for full product names)

fairly quickly but required a reboot of the system to finish off.

The main interface is a little unusual, being mainly focused on providing status information, with the few controls relegated to a minor position at the bottom of the main window. For a corporate product it seems rather short on options. For example, it appears to be impossible to check any more than the standard list of file extensions on access

– but it is possible that some additional controls may be available via some central management system.

Given our past experiences of the unreliable logging system, all large scans were run using the integrated command-line scanner. Nevertheless, we found the GUI fairly flaky under pressure, with the on-access tests against large infected sets leaving the product in something of a state, and on-demand scan options apparently left completely unresponsive until



(Please refer to text for full product names)

after a reboot. The scans of clean sets also appeared to be reporting rather small numbers of files being scanned, implying that

perhaps large numbers were being skipped for some reason (possibly due to the limited extension list). On access, however, some impressive speeding up of checking known files was observed, hinting that the product may indeed be as fast and efficient as it seemed. Resource usage measures were fairly light.

Of course, many of the tests we run present considerably more stress than would be expected in a normal situation, but it is not unreasonable to expect a little more stability in a corporate-focused product. These issues aside, we managed to get to the end of testing without any major difficulty, and scanning speeds seemed fairly decent (if they can be trusted). Detection rates were unexceptionable though, with impressive scores across the board, and with no problems in the WildList or clean sets *F-Secure* earns another VB100 award.

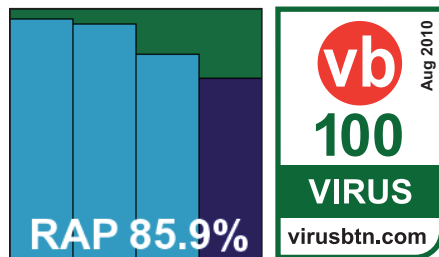
F-Secure PSB Workstation Security 9.00 build 149

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	96.48%
Worms & bots	97.80%	False positives	0

The second of *F-Secure*'s products this month has a slightly larger installer, at 69MB, but uses the same updater and has a pretty

similar set-up process and user interface. Speeds on demand were also similar, although on-access times were noticeably faster and resource usage considerably heavier – to the extent that we had to double-check the results columns hadn't been misaligned with different products. Once again the main detection tests were run with a command-line scanner for fear of the logging issues noted in previous tests.

Detection rates were just as solid as the other product, with an excellent showing and no problems in the core

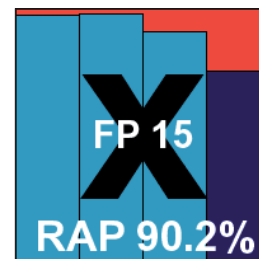


certification sets, earning *F-Secure* a second VB100 pass this month.

G DATA AntiVirus 2011 21.0.2.1

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.02%
Worms & bots	98.18%	False positives	15

G DATA's latest version, fresh and ready for next year, came as a sizeable 211MB installer, including all required updates. The installation process went through quite a few steps, including details of a 'feedback initiative' and settings for automatic updating and scheduled scanning. A reboot was needed at the end.



The new version looks pretty good, with a simple and slick design which met with general approval from the lab team. Indeed we could find very little to criticize at all, although some delving into the comprehensive configuration system did yield the information that the on-access scanner ignores archives over 300KB by default (a fairly sensible compromise, which is most likely responsible for some samples in our archive depth test being skipped). At the end of a scan, the GUI insisted on us clicking the 'apply action' button, despite us having set the default action to 'log only', and it wouldn't let us close the window until we had done this.

Scanning speeds were not too bad in the 'cold' run, and powered through in remarkable time once files had become familiar. Similar improvements were noted on access, with fairly slow initial checks balanced by lightning fast release of files once known to be safe, and resource usage was fairly sizeable but remained pretty steady through the various measures. Of course, detection rates were superb as always, with very little missed in the main sets and a stunning showing in the RAP sets. With everything looking so good, we were quite upset to observe a handful of rare false alarms in the clean sets – the same PDFs alerted on by one of the engine providers' own products – which denied *G DATA* a VB100 award this month despite an otherwise awesome performance.

Ikarus virus.utilities 1.0.214

ItW	100.00%	Polymorphic	79.99%
ItW (o/a)	100.00%	Trojans	90.36%
Worms & bots	98.70%	False positives	0

Ikarus returns to the VB100 test bench hoping for its first pass after a number of showings that have been marred by minor

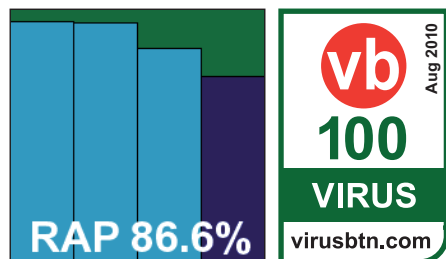
issues. The product was provided as usual as an ISO image of a CD installer, weighing in at a hefty 200MB with an additional 77MB of updates, but the initial set-up process is fast and simple. Post-install, with no reboot required, a few further set-up steps are needed, including configuring network settings and licensing, but nevertheless things are all up and running in short order. The .NET-style interface remains fairly simplistic, with few options and very little at all related to the main anti-malware functions, logging and updating taking up much of the controls.

Tests zipped through fairly nicely, with good speeds on demand but on-access times were a little on the slower side, and while CPU drain was above average, RAM usage was fairly low. As usual, the interface developed some odd behaviours during intense activity (on-demand scans provided no indication of progress, and our jobs could only be monitored by whether or not the GUI flickered and spasmed as a sign of activity). However, detection rates were solid and hugely impressive, as in several previous tests, with a particularly stunning showing in the RAP tests, and the WildList was handled impeccably despite the large numbers of polymorphic samples which have proven problematic in the past. The clean sets brought up a single alert, but as this warned that a popular IRC package was an IRC package and thus might prove a security risk, this was not a problem under the VB100 rules. After many sterling attempts, *Ikarus* thus finally earns its first VB100 certification – many congratulations are in order.

K7 Total Security 10.0.0040

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	85.81%
Worms & bots	93.81%	False positives	0

K7's compact 52MB installer package runs through its business in double-quick time, with only a few basic steps and no reboot needed. Its interface is clear, simple and easy to navigate with a logical grouping of its various components, plenty of information and a pleasing burnt orange hue. Stability was generally solid, although the interface displayed some tendency to 'go funny' after more



demanding scans – however, it recovered quickly and displayed no interruption in protection.

Scanning speeds were fairly average, and access lag fairly low, with very low resource usage. Detection rates in the main sets were pretty solid. RAP scores were slightly less impressive but still more than decent, and with no problems in the WildList and no false alarms in the clean set, another VB100 award heads *K7*'s way.

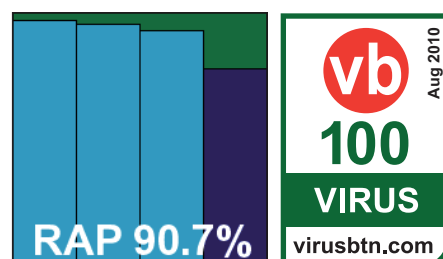
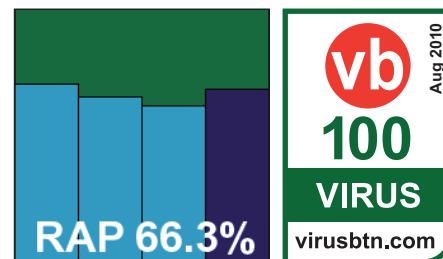
Kaspersky Anti-Virus 6.0 for Windows Workstations 6.0.4.1212

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	93.79%
Worms & bots	97.71%	False positives	0

Kaspersky once again submitted a pair of products this month, with version 6 being the more business-focused of the

two. The MSI installer package weighed in at a mere 63MB, although a multi-purpose install bundle was considerably larger, and installed fairly quickly and simply. A reboot and some additional set-up stages – mainly related to the firewall components – added to the preparation time.

Testing tripped along merrily for the most part, with some excellent speed improvements in the 'warm' scans, and on-access times were in the mid-range, with some very low RAM usage and slightly higher use of CPU cycles when busy. After large on-demand scans, logging proved something of an issue – large logs were clearly displayed in the well-designed and lucid GUI, but apparently impossible to export; a progress dialog lurked a small way in for several hours before we gave up on it and retried all the scans in smaller chunks to ensure usable results. These scores in the end proved thoroughly decent across the board, with no issues encountered in handling the required certification sets, and a VB100 award is granted to *Kaspersky Lab*'s version 6.



File access lag time (s/MB)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	11.21	0.10	NA	40.66	1.17	40.66	99.61	14.08	99.61	109.79	3.40	109.79
AhnLab V3	13.78	13.83	NA	24.06	23.74	24.06	56.28	55.96	56.28	54.40	53.91	54.40
Avast! Free	5.86	0.05	77.96	11.70	0.00	14.91	19.75	0.00	25.06	19.27	0.00	22.87
AVG IS	2.33	1.25	8.04	43.66	8.75	4.81	65.76	33.40	29.67	91.19	32.44	37.69
Avira AntiVir	5.30	2.11	31.33	12.07	0.14	13.40	28.83	17.97	31.07	30.81	29.72	32.04
BitDefender	5.22	0.24	121.75	25.36	0.00	36.41	6.43	1.54	6.36	65.34	62.62	64.48
Bkis Gateway	7.36	7.22	NA	178.23	177.12	178.23	117.43	117.36	117.43	159.60	159.50	159.60
Bkis Home	7.16	7.15	NA	179.69	187.01	179.69	116.64	116.44	116.64	158.01	156.13	158.01
Bkis Pro	7.08	7.15	NA	177.74	178.23	177.74	119.61	118.72	119.61	223.35	222.49	223.35
CA ISS Plus	7.40	7.43	NA	22.92	22.24	22.92	38.49	34.45	38.49	26.23	19.58	26.23
CA TM	6.82	6.77	NA	18.90	21.01	18.65	26.39	26.60	26.15	47.49	45.62	45.91
Central Command Vexira	2.73	2.72	7.18	33.63	32.55	31.46	39.01	37.29	48.16	118.71	118.71	127.19
Check Point Zone Alarm	4.13	0.00	NA	21.78	0.93	21.78	57.86	57.67	57.86	79.14	77.17	79.14
Coranti Multicore	14.54	14.53	24.72	140.72	136.09	135.27	214.62	213.11	241.21	249.95	247.74	293.14
Defenx Security Suite	11.59	0.00	NA	43.33	0.49	42.90	110.36	11.07	107.50	158.44	46.29	154.34
Digital Defender	2.72	2.74	58.26	65.80	65.40	64.76	4.24	4.17	33.28	39.44	38.57	89.09
eEye Blink	4.92	4.72	491.12	60.61	58.66	59.96	161.07	161.12	160.76	192.09	192.33	190.70
Emsisoft Anti-Malware	162.63	0.00	NA	386.15	0.07	386.15	2464.83	0.31	2464.83	4697.43	0.00	4697.43
eScan ISS	2.51	0.00	130.22	27.80	0.00	29.05	47.86	0.00	21.94	11.08	0.00	26.74
ESET NOD32	2.03	2.03	NA	7.05	7.05	7.05	62.23	62.01	62.23	44.43	44.18	44.43
Filseclab Twister	3.12	2.49	NA	59.50	56.75	NA	86.40	84.19	NA	83.45	82.69	NA
Fortinet FortiClient	11.38	9.09	11.38	106.24	104.08	106.24	242.74	250.52	242.74	208.10	207.24	208.10
Frisk F-PROT	8.17	8.30	NA	22.90	22.91	22.90	126.45	125.59	126.45	120.42	120.24	120.42
F-Secure Client Security	131.88	0.75	NA	98.81	0.62	NA	63.96	2.73	NA	95.86	0.00	NA
F-Secure PSB	5.31	5.52	NA	51.37	51.49	NA	14.94	14.90	NA	15.36	14.83	NA
G DATA	61.25	0.68	416.69	58.69	2.45	67.99	108.89	9.30	117.22	143.95	3.52	146.55
Ikarus virus.utilities	33.63	33.12	NA	51.47	49.97	51.47	35.03	33.36	35.03	81.03	78.77	81.03

(Please refer to text for full product names)

Kaspersky Internet Security 2011 11.0..400

ItW	100.0%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	90.84%
Worms & bots	96.56%	False positives	0

Excited to see the 2011 edition of *Kaspersky's* product, we quickly started work on the 103MB installer, with its own similarly large update bundle, which tripped along quickly with no need to reboot. The new interface sports a rather sickly pale-green hue and has some quirks, but is mostly well thought out and simple to use once it has become familiar.

Again scanning speeds were helped by excellent caching of known results – slightly slower initially than the version 6 product and

with not quite as remarkable speed-ups on second viewing of files, but on-access times were fairly similar, and in the performance measures CPU use had decreased notably at the expense of a small increase in memory use. In the infected sets some considerable wobbliness was observed, with whiting-out and crashing of the interface during scanning and once again some difficulties saving logs. Detection scores were superb however, with very little missed, and with no problems in the core sets *Kaspersky* earns a second VB100 award this month.

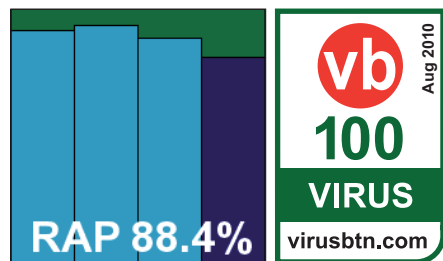
Keniu Antivirus 1.0.0.1062

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	91.17%
Worms & bots	96.53%	False positives	0

Another newcomer to our tests, Chinese developer *Keniu* provided version 1 of its product. An install package labelled 'beta'

and some as yet untranslated areas of the interface (notably the EULA) hinted that the product is at a fairly early stage of development. Based on the *Kaspersky* engine, the product was provided as a 76MB install package, which ran through simply and, despite a 20-second pause to 'analyse the system', was all done in under a minute, no reboot required.

The interface is simple, bright and breezy, with large buttons marking the major functions and a limited but easy-to-use set of options. On-demand speeds were fairly slow, but on-access times not bad at all, while performance measures were fairly hefty. In the detection sets we had a few issues, with logs trimmed to miss off the ends of longer file paths, despite the GUI claiming to have exported logs 'completely'. In the on-access tests we noticed the product getting heavily bogged down if left going for too



long. Files seemed to be being processed extremely slowly after being left over a weekend and detection had clearly stopped working some time and several thousand samples before we eventually gave up on it. By re-running this in smaller chunks, and piecing logs back together based on unique elements in the paths, we were able to obtain some pretty decent results, as expected from the quality engine underlying things. Without any problems in the clean sets and with a clear run through the WildList, *Keniu* earns its first VB100 award despite some teething problems when the product is put under heavy stress.

Kingsoft Internet Security 2011 Advanced 2008.11.6.63

ItW	99.99%	Polymorphic	58.88%
ItW (o/a)	99.99%	Trojans	15.05%
Worms & bots	47.67%	False positives	0

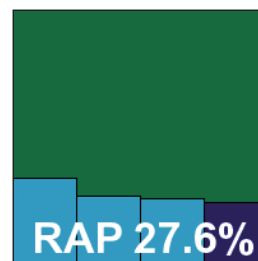
Kingsoft returns to the fray with its usual pair of near-identical products. The 'Advanced' edition was provided fully updated as a 51MB installer package, which zipped through quickly and simply and needed no reboot to complete. Controls are similarly simple and quick to navigate and operate, and what the product

lacks in glossy design it usually makes up for in generally good behaviour. Speed tests were no more than reasonable, with no sign of advanced caching of known results; RAM usage was fairly low though, and CPU use even lower, with some fairly light impact on file accessing too. On a few occasions some dents in the smooth veneer were observed, notably when scanning the system drive, it seemed to get stuck scanning a constantly growing log, and a single file in the RAP sets seemed to trip the product up too, bringing scan runs to an abrupt halt with no notification or information.

Detection rates were generally fairly meagre, and although there were no false positives in the clean set, some of the many replicated samples of W32/Virut in the WildList set proved too much, and with a fair number of misses representing one strain *Kingsoft's* 'Advanced' edition is denied a VB100 award this month.

Kingsoft Internet Security 2011 Standard 2008.11.6.63

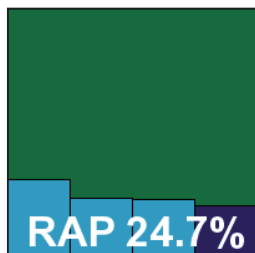
ItW	99.99%	Polymorphic	58.88%
ItW (o/a)	99.99%	Trojans	12.22%
Worms & bots	44.56%	False positives	0



File access lag time (s/MB) contd.	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
K7 Total Security	14.26	0.56	NA	57.98	0.45	57.98	27.00	3.04	27.00	92.89	40.22	92.89
Kaspersky AV 6.0	3.91	0.49	NA	35.98	0.97	35.98	64.18	4.62	64.18	94.34	0.00	94.34
Kaspersky IS 2011	4.74	0.67	26.23	34.68	0.57	34.12	67.57	3.02	70.66	96.17	0.00	100.97
Keniu Antivirus	6.74	1.27	NA	33.48	3.07	33.48	83.43	17.41	83.43	115.71	12.82	115.71
Kingsoft IS Adv.	4.86	2.63	NA	24.30	2.15	24.30	106.02	4.30	106.02	34.98	0.00	34.98
Kingsoft IS Std.	2.74	-0.35	NA	21.29	0.16	21.29	104.41	0.58	104.41	34.35	0.00	34.35
Lavasoft Ad-Aware Pro	0.99	0.85	NA	64.24	44.12	NA	3.79	3.58	NA	281.63	111.43	NA
Lavasoft Ad-Aware TS	64.95	0.68	410.19	61.24	2.60	65.35	120.76	7.57	121.83	220.60	55.63	212.42
McAfee TP	3.46	0.34	NA	34.39	1.27	34.39	18.62	3.31	18.62	127.02	0.00	127.02
McAfee VirusScan	3.62	2.13	339.90	50.04	22.14	50.74	91.54	44.26	93.10	134.49	61.46	135.35
Microsoft Security Essentials	3.77	0.48	NA	51.38	0.57	51.38	29.79	2.38	29.79	93.67	56.64	93.67
Nifty Security24	5.84	0.19	NA	30.69	1.13	30.69	75.42	7.77	75.42	135.62	35.92	135.62
Norman Security Suite	5.38	5.31	NA	63.16	63.14	63.16	168.88	167.21	168.88	199.88	199.67	199.88
PC Tools IS	2.89	1.55	NA	76.45	21.72	NA	104.59	104.65	NA	149.94	149.24	NA
PC Tools SD	3.24	1.84	NA	73.27	21.12	NA	100.78	100.60	NA	113.07	111.74	NA
Preventon Antivirus	2.36	2.35	59.70	64.10	64.02	64.82	2.93	2.49	32.30	3.24	3.01	56.16
Proland Protector Plus	1.11	0.65	3.55	31.19	7.84	31.89	11.26	10.47	55.89	63.72	63.57	134.17
Qihoo 360	2.56	1.84	NA	2.14	0.68	NA	4.58	2.43	NA	53.64	45.80	NA
Quick Heal AV	42.87	43.54	NA	15.44	15.61	15.44	73.22	74.88	73.22	71.55	71.43	71.55
Returnil RVS	21.79	21.72	NA	57.28	56.81	57.28	122.12	119.89	122.12	48.83	49.13	48.83
Rising IS	9.69	11.04	NA	81.90	54.12	81.90	163.75	164.08	163.75	142.56	143.01	142.56
Sophos Endpoint	2.39	2.44	5.58	65.10	64.79	64.70	5.07	4.65	32.21	70.46	69.74	114.20
SPAMfighter VIRUSfighter	1.87	1.99	345.95	61.53	100.46	65.87	27.47	26.91	34.63	118.34	117.60	127.88
Sunbelt VIPRE	3.13	2.65	NA	32.94	6.05	32.94	320.56	11.97	320.56	272.94	73.75	272.94
Symantec Endpoint Security	6.45	5.30	NA	63.44	62.42	63.44	63.78	60.62	63.78	58.37	55.28	58.37
Trustport AntiVirus	17.45	1.24	714.86	83.09	2.55	99.73	136.62	34.36	158.64	269.10	69.89	303.66
VirusBuster Pro	2.33	2.38	4.88	31.47	31.48	31.42	35.98	35.99	49.28	55.57	55.83	67.85

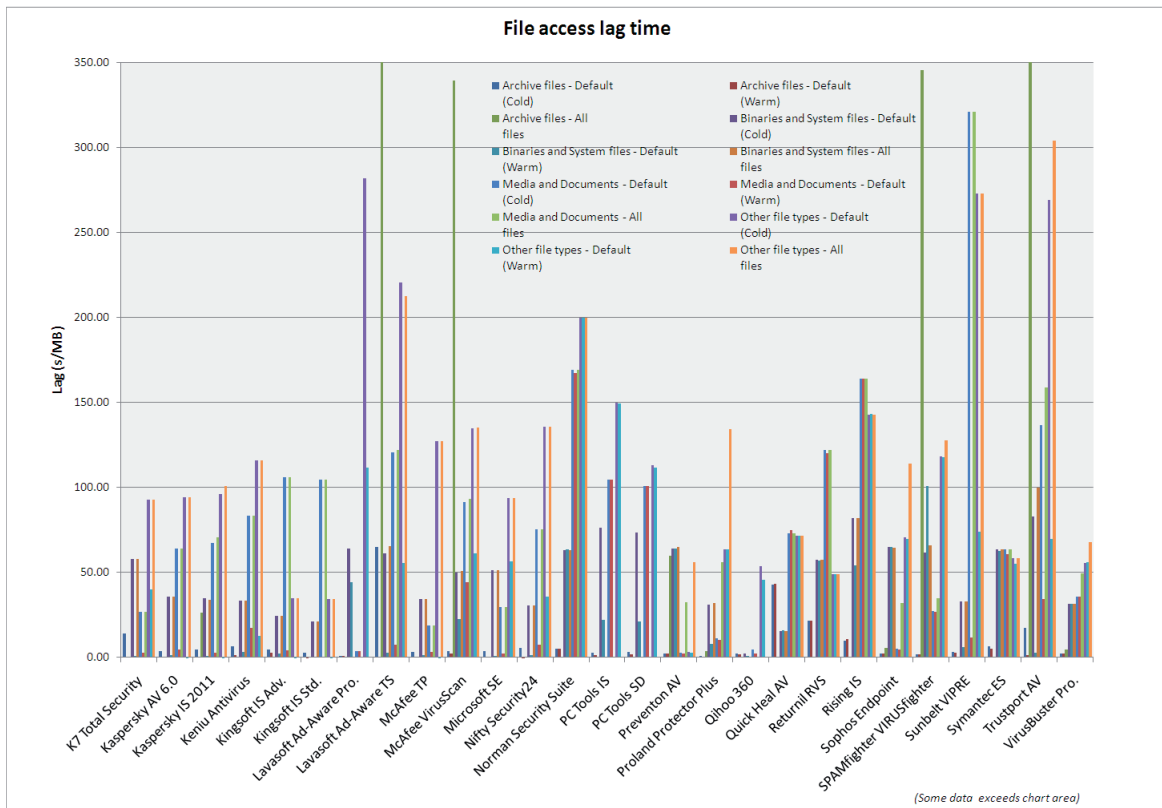
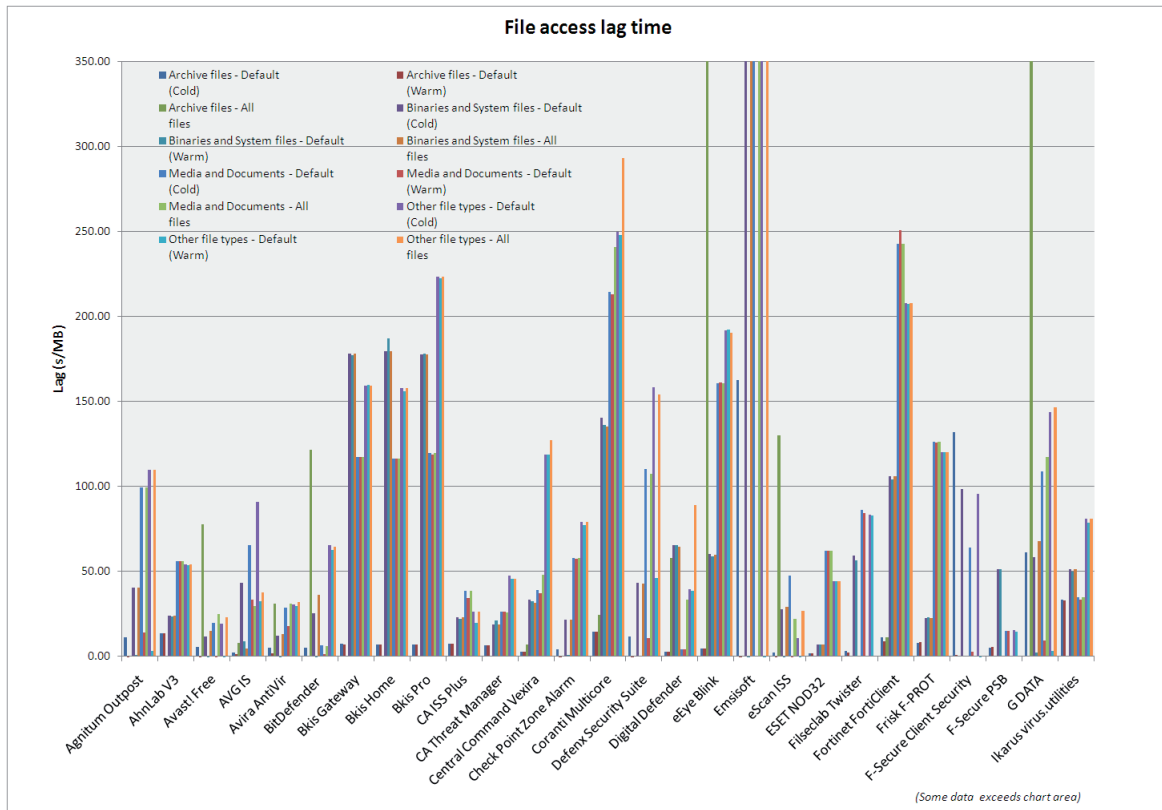
(Please refer to text for full product names)

With identical versioning and appearance, but a slightly smaller installer (at 46MB), *Kingsoft's* Standard edition is pretty hard to tell apart from the Advanced version. The set-up process, user experience and scanning speeds were all-but-



identical to those of its sibling; performance measures were closely matched too.

Detection rates were similarly on the low side, with the same issues in the system drive and RAP sets. Once again, there were no false positives generated in the clean set, but again a handful of Virut samples went undetected in the WildList set, meaning that no VB100 award can be granted.



(Please refer to text for full product names)

Lavasoftware Ad-Aware Professional Internet Security 8.3.0

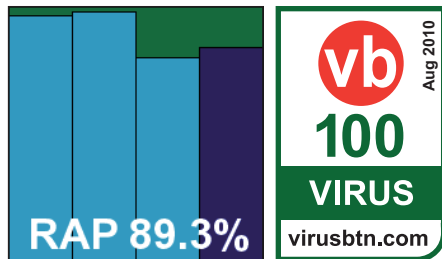
ItW	100.00%	Polymorphic	73.53%
ItW (o/a)	100.00%	Trojans	94.90%
Worms & bots	98.10%	False positives	0

The first of a pair of products from Lavasoftware, this one is the company's standard product, closely resembling those entered in a few previous

comparatives. The fairly large 137MB installer came with all required updates and installed fairly rapidly, although one of the screens passed through along the way seemed to be entirely gibberish. It also offered to install Google's Chrome browser, but skipping this step got the whole install completed in under a minute, including the required restart.

The interface was more or less unchanged from when we have encountered it on previous occasions – like several others this month it is starting to look a little plain and old-fashioned in the glitzy surroundings of a trendy modern desktop environment. However, it proved reasonably simple to navigate, providing a bare minimum of options and with a rather complex process for setting up custom scans; most users will be satisfied with the standard presets provided.

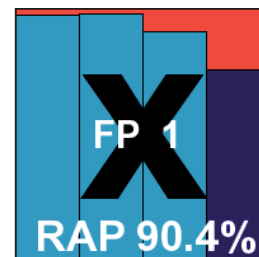
Some reasonable speeds were recorded in the clean sets, with fairly slow scan times and above average resource use, while the light on-access overheads can in part be explained by the limited range of items being checked. In the infected sets things were a little more troublesome, with scans repeatedly stopping silently with no error messages, the GUI simply disappearing as soon as we turned our backs. Fortunately, details of progress were being kept in a log entitled 'RunningScanLog.log', and after making numerous, ever-smaller runs over portions of our sets we eventually gathered a pretty much complete picture. Piecing this back together, we found no issues in the clean sets, and the WildList was handled well on demand. Running through again on access, however, we saw a handful of items being allowed to be opened by our testing tool. Investigating this oddity more closely, we found that these items had been noted in the product log, and promptly deleted when the product was set to auto-clean, thus making for a clean showing and earning Lavasoftware its first VB100 award, despite a few lingering issues with stability under heavy stress.



Lavasoftware Ad-Aware Total Security 21.1.0.28

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.21%
Worms & bots	98.24%	False positives	1

The second of Lavasoftware's offerings this month came as something of a surprise, the bulky 397MB installer marking it out immediately as a somewhat different kettle of fish from the standard solution. The set-up runs through a large number of steps, including an initial check for newer versions and the option to add in some extras, including parental controls and a secure file shredder, which are not included by default. A reboot is needed to complete, and then it spends a few moments 'initializing' at first login.



All of this had a vaguely familiar air to it, and once the interface appeared a brief look around soon confirmed our suspicions, with the GUI clearly based on that of G DATA – even down to the G DATA name appearing in a few of the folders used by the product. Testing zipped through, helped as expected by some very impressive speed improvements over previously scanned items; the only thing slowing us down was a rather long pause opening the browser window for on-demand scans, but as regular users wouldn't be running lots of small scans one after the other from the interface this is unlikely even to be noticed by the average user.

Detection rates are more important though, and the product stormed through our sets leaving an awesome trail of destruction. However, once again those pesky PDF files from Corel were alerted on in the clean set, and this stroke of bad luck keeps Lavasoftware from picking up a second VB100 this month.

McAfee Total Protection 10.5 (610.5.178)

ItW	99.99%	Polymorphic	99.99%
ItW (o/a)	99.99%	Trojans	87.19%
Worms & bots	94.68%	False positives	0

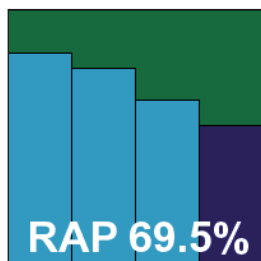
McAfee's home-user product has taken part in a few comparatives of late, but familiarity hasn't made it any more popular with the lab team. The installation process is entirely online, with a tiny 2.9MB starter file pulling down all the required components from the web. This amounted to some 116MB and took a good five minutes to pull down; it installed with reasonable promptness and without

Product	RAM use increase - idle system	RAM use increase - heavy file access	CPU use increase - heavy file access
Agnitum Outpost	10.42%	10.43%	21.76%
AhnLab V3	7.88%	5.87%	34.95%
Avast! Free	8.74%	8.55%	19.44%
AVG IS	12.28%	11.96%	42.62%
Avira AntiVir	8.77%	7.57%	16.14%
BitDefender	7.11%	5.29%	0.02%
Bkis Gateway	16.49%	16.75%	58.70%
Bkis Home	12.79%	12.95%	54.78%
Bkis Pro	20.53%	18.40%	49.69%
CA ISS Plus	33.80%	13.18%	20.81%
CA Threat Manager	9.96%	9.31%	17.26%
Central Command Vexira	10.14%	9.35%	19.30%
Check Point Zone Alarm	9.69%	12.72%	29.95%
Coranti Multicore	15.99%	15.66%	63.56%
Defenx Security Suite	10.75%	11.68%	15.61%
Digital Defender	8.20%	6.73%	34.73%
eEye Blink	12.34%	13.37%	58.59%
Emsisoft Anti-Malware	5.45%	6.32%	68.87%
eScan ISS 11	5.45%	6.73%	17.86%
ESET NOD32	4.15%	5.62%	37.12%
Filseclab Twister	35.05%	46.55%	4.60%
Fortinet FortiClient	26.28%	22.75%	25.32%
Frisk F-PROT	10.76%	5.41%	31.75%
F-Secure Client Security	6.88%	10.34%	34.86%
F-Secure PSB	32.19%	41.26%	52.27%
G DATA	35.67%	37.39%	35.84%
Ikarus virus.utilities	9.06%	8.01%	42.95%

(Please refer to text for full product names)

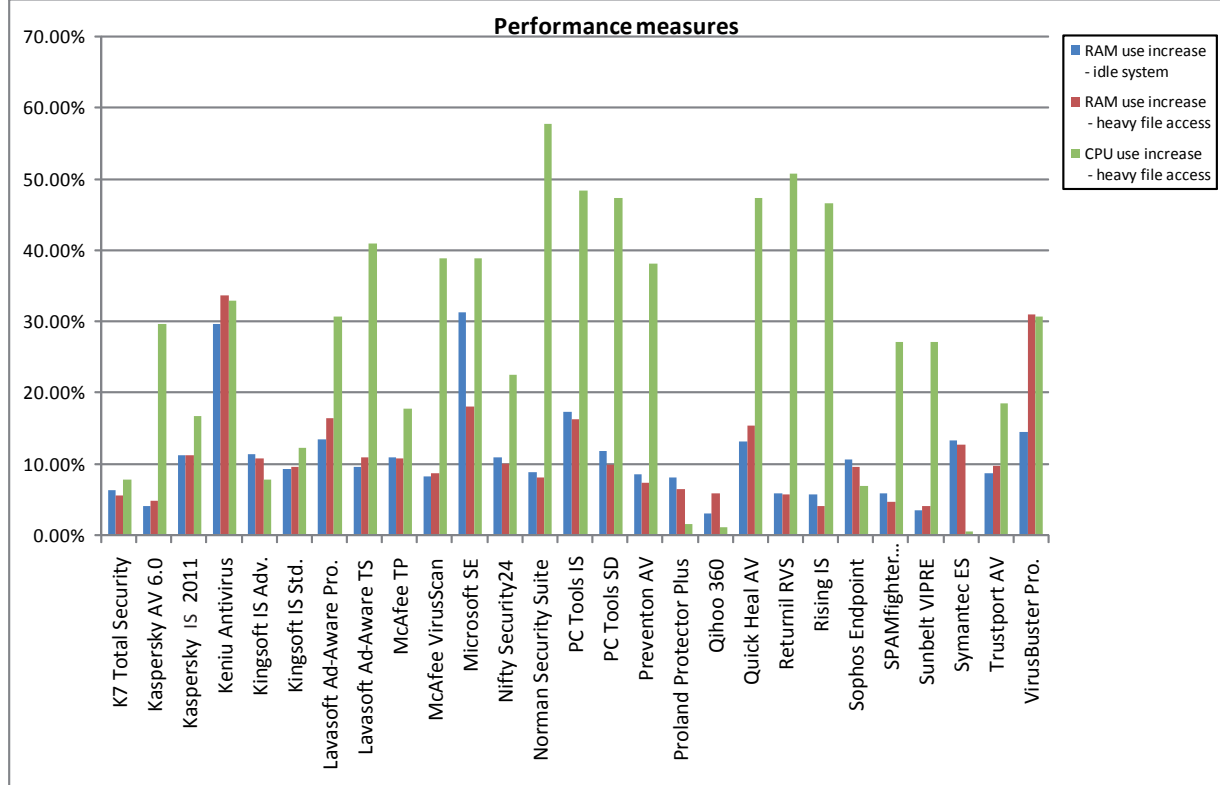
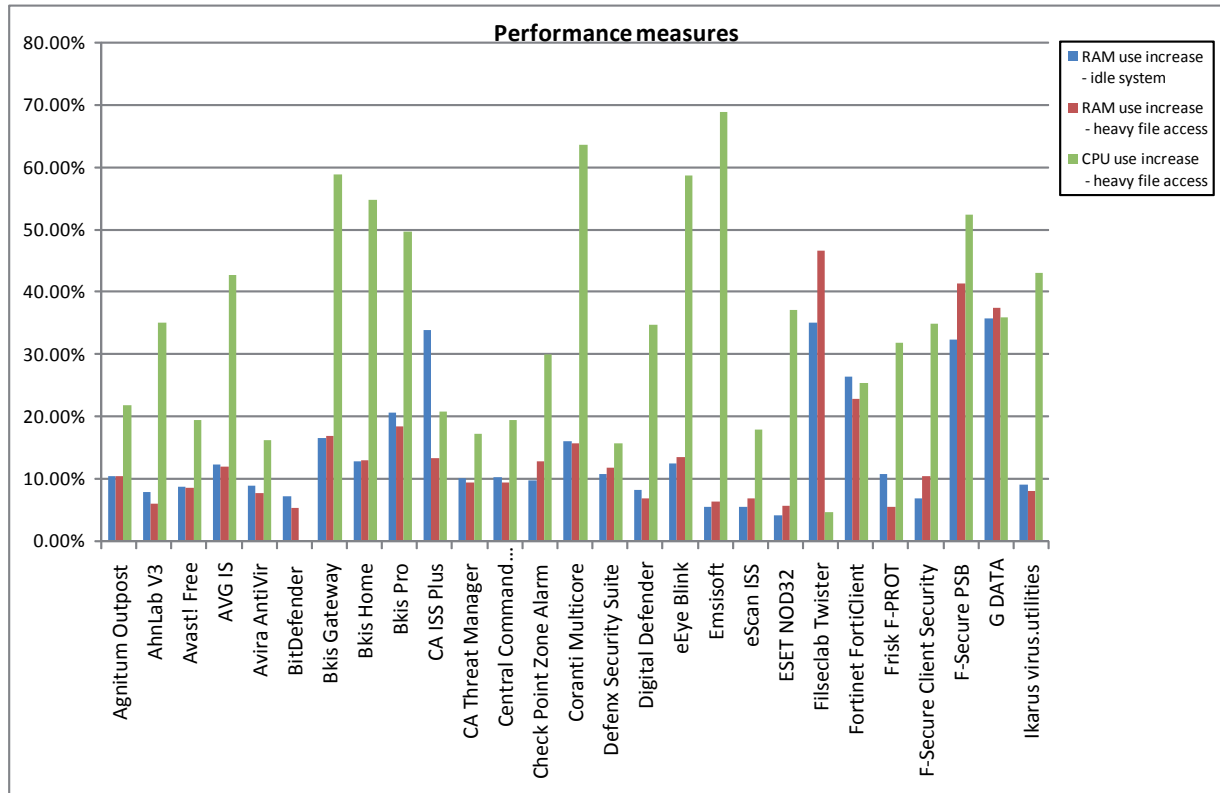
Product	RAM use increase - idle system	RAM use increase - heavy file access	CPU use increase - heavy file access
K7 Total Security	6.39%	5.71%	7.91%
Kaspersky AV 6.0	4.13%	4.88%	29.62%
Kaspersky IS 2011	11.20%	11.27%	16.71%
Keniu Antivirus	29.72%	33.64%	32.99%
Kingsoft IS Adv.	11.39%	10.80%	7.90%
Kingsoft IS Std.	9.27%	9.71%	12.24%
Lavasoft A-A Pro	13.45%	16.43%	30.71%
Lavasoft A-A TS	9.60%	10.95%	40.91%
McAfee TP	10.93%	10.82%	17.73%
McAfee VirusScan	8.24%	8.77%	38.80%
Microsoft SE	31.37%	18.15%	38.90%
Nifty Security24	11.02%	10.06%	22.57%
Norman SS	8.95%	8.12%	57.67%
PC Tools IS	17.29%	16.28%	48.40%
PC Tools SD	11.83%	9.93%	47.35%
Preventon AV	8.60%	7.45%	38.06%
Proland	8.10%	6.58%	1.60%
Qihoo 360	3.14%	5.89%	1.18%
Quick Heal AV	13.21%	15.38%	47.32%
Returnil RVS	5.93%	5.80%	50.71%
Rising IS	5.79%	4.21%	46.51%
Sophos Endpoint	10.66%	9.65%	6.96%
SPAMfighter VIRUSfighter	5.97%	4.80%	27.20%
Sunbelt VIPRE	3.60%	4.13%	27.10%
Symantec ES	13.35%	12.68%	0.64%
Trustport AntiVirus	8.79%	9.84%	18.48%
VirusBuster Pro	14.54%	30.96%	30.74%

too much effort. No reboot was needed to get protection in place. The interface manages to be ugly and awkward to operate, heavily text-based and strangely laid out. Messaging was somewhat confusing, with some areas of the interface seeming to imply that on-access



protection was disabled, while others claimed it was fully operational.

Very few options are provided for the user, and those that are available are hard to find, so our few simple needs (including recording details of the changes made to our system by the product) had to be implemented by means of adjustments in the registry. The 'custom' option for the on-demand scanner only provided options to scan whole drives or system areas, so our on-demand speed measures



(Please refer to text for full product names)

were taken using right-click scanning. Scanning speeds proved fairly reasonable, with some signs of improvement when scanning previously checked items, while on-access speeds seemed fairly zippy and resource usage was quite light.

The product crashed out after some of the larger scans of infected sets, leaving no information as to why, and of course having overwritten its own logs. We also noted that some *Windows* settings seemed to have been reset – notably the hiding of file extensions, which is one of the first things we tweak when setting up a new system. On several occasions this was found to have reverted to the default of hiding extensions, which is not only a security risk but also an activity exhibited by some malware.

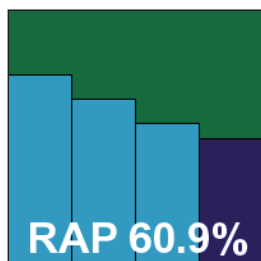
In the clean sets a VNC client was correctly identified as a VNC client, and in the infected sets scores were generally pretty decent – this would most likely be improved by the product's online lookup system, which is not available during the test runs. In the WildList set, however, a selection of Virut samples were not detected, and as a result no VB100 award can be granted to *McAfee*'s home-user offering this month.

McAfee VirusScan Enterprise 8.7.0i

ItW	99.99%	Polymorphic	99.99%
ItW (o/a)	99.99%	Trojans	80.16%
Worms & bots	92.13%	False positives	0

Leaving these troubles behind with some relief, we come to *McAfee*'s corporate product which has long been popular with the lab team for its dependability, sensible design and solidity. It kicks off its installer with an offer to disable *Microsoft*'s *Windows Defender*, which worried us a little with its lack of details on the source of the offer. The rest of the installation process, running from a 26MB installer and a 77MB update file, was fast and easy, with a message at the end stating that a reboot was only required for some components, the core protection parts being operational from the off. The GUI remains grey and drab but easy to use, logically laid out and oozing trustworthiness, providing a splendid depth of configuration (ideal for a business environment).

Scanning speeds were decent with the default settings and not bad with more thorough scanning enabled, while on-access times also went from very fast to not bad when turned up to the max. RAM usage was reasonable too, with



CPU use no higher than most this month. Detection rates were generally good, with some fairly decent RAP scores, and the clean sets were handled without issue, but again that small handful of W32/Virut samples were not detected and *McAfee*'s business solution also misses out on a VB100 award this month.

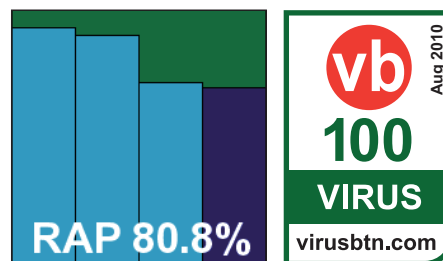
Microsoft Security Essentials 1.0.1961.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	94.29%
Worms & bots	98.34%	False positives	0

Microsoft's free solution was provided as a tiny 7MB installer with an impressively slim 55MB of updates, and installs rapidly

and easily, in a process only enlivened by the requirements of the 'Windows Genuine Advantage' programme. No reboot is needed, and with the clear and usable interface providing only basic controls, testing progressed nicely. Scanning speeds were unremarkable, with some slowish measurements on demand but fairly decent file access lags, while resource usage seemed rather on the high side. Detection rates were strong as ever, with a good showing in the RAP sets.

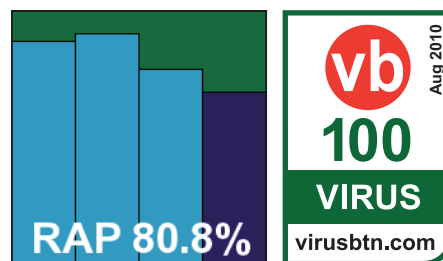
With no problems in the WildList or clean sets, *Microsoft* earns another VB100 award with ease.



Nifty Corporation Security24

ItW	100.0%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	87.80%
Worms & bots	95.80%	False positives	0

Nifty returns to the VB100 line-up to test our testing skills to the extreme. Once again untranslated from its native Japanese, and with much of the script on the interface rendered as



meaningless blocks and question marks in our version of *Windows*, navigation has never been simple, and is not helped by a somewhat eccentric interface layout.

Installation of the 178MB package (which included the latest updates) was not too tricky, with what seemed to be the standard set of stages for which the 'next' button was easy to spot. One screen was rather baffling however, consisting of a number of check boxes marked only with question marks, except for the words 'Windows Update'. We soon had things up and running though, after an enforced reboot and, aided by previous experience and some tips from the developers, got through the test suite fairly painlessly.

Scanning speeds were pretty decent, helped out by the zippy 'warm' scans which are a trademark of the *Kaspersky* technology underlying the product, while resource usage was fairly average. The on-access detection tests went pretty smoothly, but the on-demand scans of infected sets took rather a long time. Logging seemed only to be available from the *Windows* event viewer, which of course had to be set not to abandon useful information after only a few minutes of scanning. Over time, large scans of infected sets seemed to slow down to a snail's pace, and with time pressing, RAP scores could only be gathered on access. This may result in some slightly lower scores than the product is truly capable of, with additional heuristics likely to come into play on demand to explain the slowdown, but when less than a third of the sets had been completed after five days, it seemed best to provide at least some data rather than continue waiting.

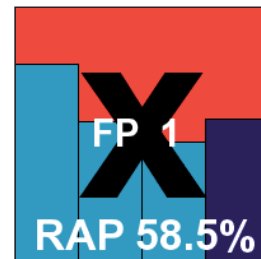
Eventually results were gathered for the main sets, which showed the expected solid coverage, with no more to report in the clean sets than a couple of 'suspicious' items (the usual VNC and IRC packages alerted on as potential security risks). The WildList was handled without issues either, and *Nifty* comfortably adds to its growing tally of VB100 passes.

Norman Security Suite (NVC 8.00.00)

ItW	100.00%	Polymorphic	84.02%
ItW (o/a)	100.00%	Trojans	69.85%
Worms & bots	85.24%	False positives	1

Norman's suite came as a 77MB package with all updates included, and only took a few steps and a reboot to get working, although some further set-up was needed after installation. The interface provides a basic range of options, and does so in a rather fiddly and uncomfortable manner for our tastes, but is generally well behaved and usable. On-demand scanning speeds were distinctly slow

compared to the rest of the field – presumably thanks to the sandbox component's thorough investigation of the behaviour of unfamiliar executables. Similar slowness was noted in the on-access measures, matched by high use of CPU cycles, although RAM use was not excessive.

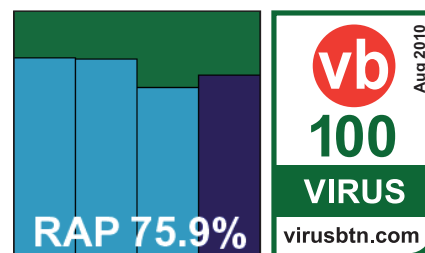


Running the high-stress tests over the infected sets caused some problems with the GUI, which lost its links to the on-demand and scheduled scanning controls several times, denying they were installed despite them continuing to run jobs. Protection seemed to remain solid however, and detection was reasonable across the board, but in the clean set a false alarm appeared, with part of *Roxio*'s DVD authoring suite once again being labelled as a Swizzor trojan, thus denying *Norman* a VB100 once again.

PC Tools Internet Security 7.0.0.545



















ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	80.29%
Worms & bots	88.89%	False positives	0

PC Tools provided its full suite solution as a 134MB installation package, which runs through with reasonable speed and



simplicity, warning at the end that a reboot may be required in a few minutes. After restarting, the interface is its usual self, looking somewhat drab and flat against the glossy backdrop of *Vista*'s Aero desktop. The layout is somewhat different from the norm, with a large number of sub-divisions to the scanning and protection, and in a quick scan of the system partition it was the only product to raise an alert – reporting a number of cookies found (each machine paid a brief visit to MSN.com to check connectivity prior to activation of the operating system, and presumably the cookies were picked up at this point).

Having grown familiar with the product during the process of a standalone review recently (see *VB*, July 2010, p.21), we suddenly found the layout a little confusing once again, failing to find some useful options and ending up having to let the product delete, disinfect and quarantine its way through the sets. Nevertheless, results were obtained without serious problems, and scanning speeds proved

Reactive and Proactive (RAP) detection scores		Reactive			Reactive average	Proactive	Overall average
		week -3	week -2	week -1		week +1	
Agnitum Outpost		84.68%	82.22%	65.20%	77.37%	57.68%	72.45%
AhnLab V3		59.64%	48.70%	33.58%	47.31%	36.18%	44.53%
Avast! Free		94.17%	93.25%	84.39%	90.60%	72.43%	86.06%
AVG IS		97.18%	95.92%	88.50%	93.87%	74.75%	89.09%
Avira AntiVir		97.46%	95.42%	88.38%	93.75%	76.63%	89.47%
BitDefender		96.07%	94.40%	84.19%	91.55%	73.12%	86.95%
Bkis Gateway		28.88%	34.32%	26.06%	29.75%	28.30%	29.39%
Bkis Home		28.88%	34.32%	26.06%	29.75%	28.30%	29.39%
Bkis Pro		28.88%	34.32%	26.06%	29.75%	28.30%	29.39%
CA Internet Security Suite Plus		77.15%	72.94%	54.15%	68.08%	52.56%	64.20%
CA Threat Manager		62.92%	61.61%	52.30%	58.94%	51.45%	57.07%
Central Command Vexira		84.84%	82.46%	65.40%	77.57%	57.53%	72.56%
Check Point Zone Alarm		90.68%	92.14%	88.99%	90.60%	78.28%	87.52%
Coranti Multicore		99.91%	99.35%	95.63%	98.30%	84.37%	94.82%
Defenx Security Suite		84.95%	82.59%	65.58%	77.71%	57.80%	72.73%
Digital Defender		82.42%	79.92%	63.03%	75.12%	55.45%	70.21%
eEye Blink		77.23%	54.75%	47.19%	59.72%	56.16%	58.83%
Emsisoft Anti-Malware		95.23%	95.08%	86.02%	92.11%	74.44%	87.69%
eScan ISS		97.42%	95.11%	86.65%	93.06%	74.53%	88.42%
ESET NOD32		94.77%	94.58%	94.63%	94.66%	77.29%	90.32%
Filseclab Twister		83.80%	79.00%	72.11%	78.30%	59.56%	73.62%
Fortinet FortiClient		72.66%	78.44%	56.68%	69.26%	47.45%	63.81%
Frisk F-PROT		82.19%	71.79%	64.97%	72.98%	68.62%	71.89%
F-Secure Client Security		95.93%	93.98%	81.70%	90.54%	72.04%	85.91%
F-Secure PSB		95.41%	93.71%	81.07%	90.07%	71.06%	85.31%
G DATA		97.23%	97.80%	90.51%	95.18%	75.34%	90.22%
Ikarus virus.utilities		94.65%	94.24%	84.09%	90.99%	73.35%	86.58%

(Please refer to text for full product names)


















fairly average but fast over the important executables sets, with similarly lightish times in the on-access speed measures and reasonably high use of RAM and CPU cycles.

Detection rates were solid, with a very steady rate in the RAP sets, and with no issues handling the clean or WildList sets *PC Tools* earns a VB100 award without difficulty.

PC Tools Spyware Doctor with Anti-virus 7.0.0.545

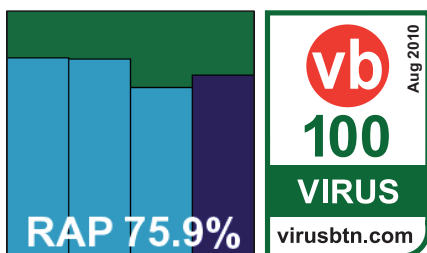
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	80.29%
Worms & bots	88.89%	False positives	0

The second of *PC Tools*' offerings this month was pretty

Reactive and Proactive (RAP) detection scores contd.		Reactive			Reactive average	Proactive week +1	Overall average
		week -3	week -2	week -1			
K7 Total Security		70.07%	65.42%	61.53%	65.68%	68.03%	66.26%
Kaspersky Anti-Virus 6.0		96.78%	95.21%	92.70%	94.89%	77.94%	90.66%
Kaspersky Internet Security 2011		91.29%	93.22%	88.23%	90.91%	80.85%	88.40%
Keniu Antivirus		91.56%	94.30%	88.30%	91.38%	73.16%	86.83%
Kingsoft IS Advanced		33.79%	26.58%	25.87%	28.75%	24.18%	27.60%
Kingsoft IS Standard		31.25%	23.52%	23.39%	26.05%	20.55%	24.68%
Lavasoft Ad-Aware Professional		96.02%	97.56%	80.00%	91.19%	83.41%	89.25%
Lavasoft Ad-Aware Total Security		97.38%	97.92%	90.79%	95.36%	75.59%	90.42%
McAfee Total Protection		82.96%	76.69%	64.36%	74.67%	54.06%	69.52%
McAfee VirusScan		74.10%	64.96%	55.42%	64.83%	49.25%	60.93%
Microsoft Security Essentials		92.62%	89.86%	71.42%	84.64%	69.33%	80.81%
Nifty Security24		87.71%	90.75%	76.89%	85.12%	67.95%	80.83%
Norman Security Suite		77.22%	54.52%	46.60%	59.45%	55.78%	58.53%
PC Tools IS		80.65%	80.39%	69.00%	76.68%	73.72%	75.94%
PC Tools Spyware Doctor		80.65%	80.39%	68.99%	76.68%	73.72%	75.94%
Preventon Antivirus		82.42%	79.92%	63.03%	75.12%	55.45%	70.21%
Proland Protector Plus		83.25%	83.32%	71.13%	79.23%	70.36%	77.01%
Qihoo 360		96.33%	94.84%	86.92%	92.69%	73.97%	88.01%
Quick Heal AntiVirus		74.21%	76.31%	58.39%	69.64%	51.18%	65.02%
Returnil RVS		80.65%	69.36%	67.46%	72.49%	69.86%	71.83%
Rising IS		60.82%	51.33%	56.04%	56.06%	39.55%	51.94%
Sophos Endpoint		85.03%	82.13%	77.89%	81.68%	70.43%	78.87%
SPAMfighter VIRUSfighter		82.25%	79.05%	59.45%	73.58%	54.18%	68.73%
Sunbelt VIPRE		95.86%	97.46%	70.51%	87.95%	83.19%	86.76%
Symantec Endpoint Security		77.42%	75.89%	57.16%	70.16%	53.76%	66.06%
Trustport AntiVirus		97.74%	98.33%	97.14%	97.74%	80.91%	93.53%
VirusBuster Professional		79.74%	76.95%	58.46%	71.71%	53.02%	67.04%

(Please refer to text for full product names)

similar to the first, but lacked a firewall and some other functions, and notably had some components of the multi-faceted



'Intelli-guard' system disabled in the free trial mode. The core parts, including standard filesystem anti-malware protection, were fully functional however. The installer was thus slightly smaller at 129MB, but the set-up process was similarly quick and to-the-point, with no restart needed this time.

The interface proved no problem to navigate – perhaps thanks to practice gained testing the previous product.

We felt that a little was left to be desired in the area of in-depth options but everything we needed was to hand. Having become rather exhausted by the unending barrage of products by this point, we welcomed a little light relief in the form of the product's cartoon logo – in which we have noted before that the 'Doctor' actually resembles a large glass of cold beer more than anything. One other quirk of the product is that in order for it to keep its detection logs intact it needs to be disconnected from any networks, otherwise it tries to send them out into space for feedback purposes.

The tests tripped along merrily without upset or any sign of instability even under heavy pressure, and again performance measurements were fairly decent if not exceptional. Likewise, detection rates were solid and reliable without being flashy. With no problems in the core certification areas, a second VB100 goes to *PC Tools* this month, along with our gratitude for a relatively painless testing experience.

Preventon Antivirus 4.2.37

ItW	99.84%	Polymorphic	89.73%
ItW (o/a)	99.84%	Trojans	80.71%
Worms & bots	88.44%	False positives	0

Preventon's compact 48MB installer zips along rapidly, a highlight being the extensive list of available languages including Danish and Dutch. No reboot is needed to get things up and working. The now-familiar interface is delightfully simple and packs a good level of controls into a small area, although much of this is available only to 'pro' users, with a fully licensed product.

On-demand speeds were somewhat mediocre, but file access lag times were not too intrusive, while RAM use was medium and CPU slightly above average. Detection rates were decent in general, with no false alarms; however, a single Ircbot sample in the WildList set was not detected, and *Preventon* therefore misses out on a VB100 award this month.

Proland Protector Plus 9.1.006

ItW	100.00%	Polymorphic	89.73%
ItW (o/a)	100.00%	Trojans	80.88%
Worms & bots	91.17%	False positives	0

Proland's 69MB install package goes about its business in a short and sweet fashion, the brief set-up process enlivened

by the unusual but thoughtful offer to add a support contact to the *Windows* address book. Protection is in place in short order with no

reboot required, and the main interface is bright and brisk with a nice simple layout that makes for easy use.

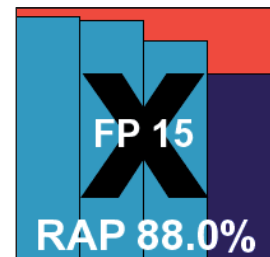
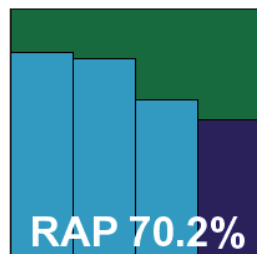
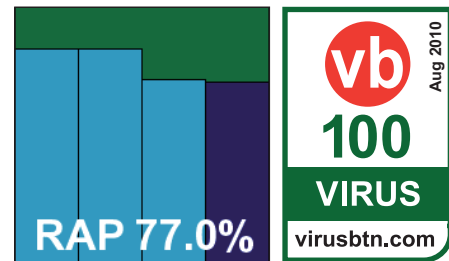
Scanning speeds were reasonable, with decent on-access speeds and remarkably low resource usage, with CPU drain barely registering. Detection rates were similarly decent, closely matching those of other products based on the *VirusBuster* engine. With the clean set handled nicely and no issues with the WildList item which upset a few fellow users of the *VirusBuster* engine, *Protector Plus* proves worthy of another VB100 award.

Qihoo 360Security 1.1.0.1309

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	97.78%
Worms & bots	98.53%	False positives	15

Qihoo has had a clean run in its first couple of VB100 entries, and returns this month hoping for a third award. The product, kindly translated into English after an initial entry which only supported the company's native Chinese, came as a 91MB install package with all updates included, and was set up in no time, with a bare minimum of steps, few options to tax the brain and no reboot needed. On opening the interface, options to make use of online 'cloud' protection and to join a feedback system are offered. Users are also urged to install '360 Security Guard' for additional protection.

The interface itself is smooth and simple with a sensible, logical layout, and provides a good level of configuration controls. Scanning speeds were not hugely impressive, but at least consistent, but on-access times were very swift and resource consumption very low. By default, the product only monitors 'applications' on access, and despite enabling an option to scan all files we saw no detection of the Eicar test file with a randomly chosen extension. Detection rates were solid across the board, with some excellent RAP scores, and the WildList caused no



problems, but in the clean sets once again a selection of items, all contained in a single install package from *Corel*, were flagged as containing PDF exploits, spoiling *Qihoo*'s run of good fortune and denying the vendor a VB100 award this month.

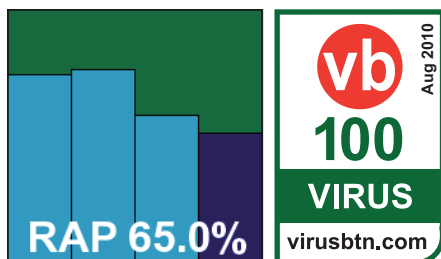
Quick Heal AntiVirus 2010 11.00 (4.0.0.3)

ItW	100.00%	Polymorphic	99.94%
ItW (o/a)	100.00%	Trojans	81.82%
Worms & bots	90.09%	False positives	0

Quick Heal's solution has grown from once minimal size to a mid-range 105MB, including all updates, but still zips into place with

only simple, unchallenging queries and no reboot needed. The interface is a little confusing in places, but generally fairly easy to navigate. Scanning speeds, once remarkable, were this month no more than decent, with file access lags and resource consumption higher than expected, and some serious delays were imposed when trying to export larger scan logs.

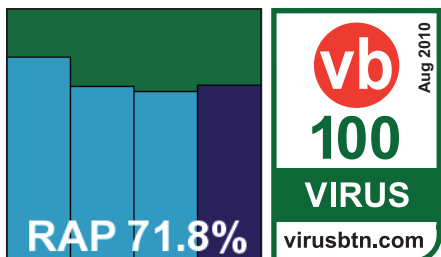
Results showed some decent scores, with on-demand detection rates notably better than on access, and RAP scores were not bad either; no issues cropped up in the WildList set or clean sets, and a VB100 award is duly granted to *Quick Heal*.



Returnil Virtual System 2010 3.2.9467.5334-RC0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	79.51%
Worms & bots	90.13%	False positives	0

Returnil has been working up to inclusion in a VB100 comparative review for a few months now, and we've looked forward to finally welcoming the vendor to the fold. The



product, as hinted at by its title, is based on a virtualization system which allows the user to revert the system to a clean state at the click of a button – an interesting and unusual offering which we look forward to looking at in more depth in due course. For now, we mainly looked at the anti-malware component included as an extra, which is based on the *Frisk* engine.

The installer is 36MB, with an additional 22MB of updates, and runs through quite simply, with just a few simple steps and a reboot to complete. Once in place, a button lurks on the desktop to control the virtualization component. The anti-malware component is provided with a few basic options, which proved ample for our needs. It is attractive, lucid and well designed, and seemed to maintain a good level of stability during our stressful tests – although at one point in a large scan of the infected sets a crash was observed, with a warning that the Data Execution Prevention sub-system had prevented some unwanted activity; the machine had to be restarted to get things back to normal.

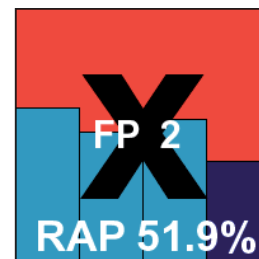
Pushing on with the tests, we witnessed some reasonable scanning speeds in the on-demand tests, and file access lags and CPU use were a little on the high side, though memory use was no more than average. In the infected sets, scores were generally pretty decent, with a remarkably steady rate in the later three weeks of the RAP sets. No problems were seen in the WildList or clean sets, and *Returnil*'s interesting and unusual product proves worthy of a VB100 award.

Rising Internet Security 22.00.04.20

ItW	100.00%	Polymorphic	70.87%
ItW (o/a)	100.00%	Trojans	55.01%
Worms & bots	63.55%	False positives	2

Rising has had a rather sporadic and unpredictable history in VB100 testing over the past few years, with an on-off pattern of entries and a similarly up-and-down record of passes and fails. The latest product came as a mid-sized 84MB package, and installation was reasonably painless, with a few standard steps plus questions about allowing *Windows* services to access the local network. After a reboot, some further configuration is provided in wizard format, with a choice of skin for the GUI notable among the options (the team selected 'Polar Dust', a pleasant black-and-blue design).

Scanning speeds were fairly mediocre, on-access lag times were heavy and CPU use was also high, although memory



was not overused. A few issues were encountered in the infected sets, with a message appearing during the biggest scan warning that 'ravmond' had stopped working – this did not appear to have affected the running scan however, and protection seemed to still be in place (or at least to have come back on again by the time we checked). When running the highly stressful on-access scan over the infected sets another issue emerged, with the whole window system turning milky white and refusing to respond; a hard reboot was needed to recover. Also adding to our problems, blocking of access does not operate in the standard manner, and the logs had to be checked to measure detection of items which our tools had been allowed to open.

Looking over the results, scores were not hugely impressive in most sets, though fairly even at least in the reactive portions of the RAP sets. In the WildList a handful of items were missed (oddly, different ones in on-demand and on-access checks). In the clean sets, a pair of false alarms were also noted, with 'Generic Trojan' alerts raised against the rather obscure software packages named *Photoshop* and *Acrobat*. *Rising* is thus denied a VB100 award this month.

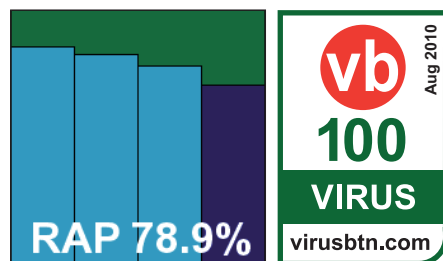
Sophos Endpoint Security and Control 9.5.0

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	88.59%
Worms & bots	88.63%	False positives	0

Sophos provided its latest version just in time for this test, with additional components in this version including 'cloud'-based

scanning and much else not covered by our current testing regime. The 81MB installer was accompanied by only 4MB of updates, and ran through in decent time, a moment of interest being the offer to remove 'third-party' (meaning competitor) products. No reboot was needed to get going, and initial tests sped through rapidly, with excellent on-demand scan times only dented by turning up archive scanning. Similarly rapid results were obtained in the on-access tests, with pretty low resource usage.

Scanning the infected sets proved considerably slower than previous experiences, but this was easily remedied by fully disabling the 'live' component and resultant online lookups. Detection rates were pretty decent, and only a

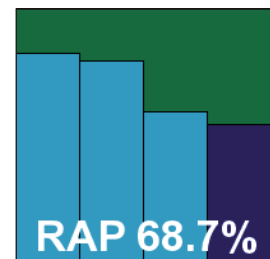


few 'suspicious' items were flagged in the clean sets. This, combined with a clean sweep of the WildList set, means that *Sophos* qualifies for another VB100 award this month.

SPAMfighter VIRUSfighter 6.102.3

ItW	99.84%	Polymorphic	89.73%
ItW (o/a)	99.84%	Trojans	80.68%
Worms & bots	88.43%	False positives	0

SPAMfighter's product is provided as a slender 49MB package and gets itself into place rapidly and easily, with just a few steps and no restart required. The GUI is adorned with an army helmet to emphasize its defensive nature, and is bright and friendly with a reasonably sensible layout providing some basic options but nothing too complex or demanding.



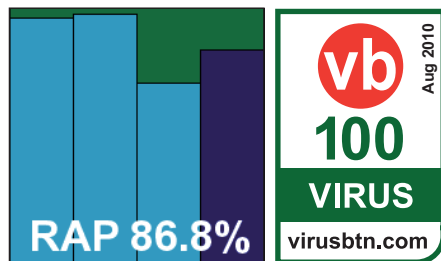
Having checked these out we rebooted the system as standard, and found on restart that the login process was rather slow; watching it for a few minutes, we saw the desktop appear but trying to click an icon made it white out, and it remained in this state for a long time. A hard reboot was needed, but after that no further problems were observed, and testing proceeded apace. On-demand speeds were not bad, while on-access lag times were fairly noticeable, with average memory consumption and not too much CPU use. Detection rates were pretty decent, with a good start in the RAP sets falling off sharply in the later weeks. The clean sets were handled nicely, but in the WildList a single Ircbot was once again missed, as with other products using the same engine, and *SPAMfighter* is denied a VB100 award this month.

Sunbelt VIPRE 4.0.3295

ItW	100.00%	Polymorphic	73.53%
ItW (o/a)	100.00%	Trojans	90.50%
Worms & bots	97.83%	False positives	0

Sunbelt's marketing campaigns regularly boast of *VIPRE's* lightness of weight and lack of bloat, and these assertions are certainly supported by the product's wafer-thin 16MB installer, supplemented by a mere 66MB of updates, available to download as a standalone package from the company's website. The set-up process is short and sweet too, taking only a few seconds to complete – with no reboot needed, the process was over in less than half a minute.

Once the interface is opened for the first time, a few set-up steps are required, including integration with mail clients, the joining of an online feedback system, and the offer of a demo video hosted online.



The interface has a pleasant and fairly simple-to-navigate design. Running through the speed tests was reasonably fast, with impressive speeds in the sets of executables and other binaries – where other products are usually slowest – but notably slower than most in the documents & media set. On-access measures reflected this pattern, and while CPU use when busy was on a par with others, RAM consumption was notably low at all times.

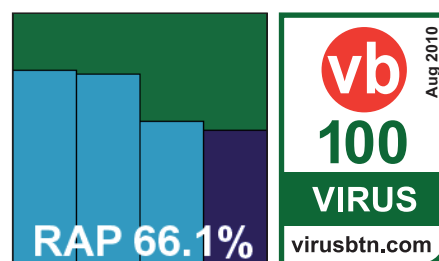
In the infected sets, a problem emerged during an overnight scan. On returning the next morning we found the scan to have snagged somewhere in the RAP sets – while the interface showed a moving progress bar, the duration timer and ‘current file’ entries remained static, and we decided to give up on it and try again in smaller chunks. This proved no easy matter, as similar problems were encountered many times, sometimes getting close to the end of a batch only to display a message saying ‘your scan has failed – if this persists please contact Technical Support’. Logging appears not to be written until a scan has successfully completed, so hours and then days were wasted in waiting for a freeze or an error message. Eventually enough data had been gathered, showing some very respectable scores in all the sets, with the rate for the trojans set slightly lower than it could perhaps have been, thanks to having to skip some folders where crashes seemed unavoidable.

The on-access test also hit a snag when all detection seemed to cease 90% of the way through the sets, and a reboot was needed to get protection back online. Again several smaller retries were needed and some sections of the trojans set had to be skipped. The clean set was handled without problems, and the WildList covered flawlessly on demand; on access the same dozen items missed by another product based on the *VIPRE* engine this month were not blocked, but checking the somewhat ephemeral logs, and retrying with deletion enabled, showed that everything was being detected, and *Sunbelt* earns another VB100 award despite having made us work extra hard and caused not inconsiderable frustration in the process.

Symantec Endpoint Security 11.0.5002.333

ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	77.40%
Worms & bots	86.44%	False positives	0

Symantec's developers entered only their corporate solution for this test, and provided it as usual as a sizeable install package. The



package included numerous additional components such as management agents and so on, making the 522MB zip file impossible to compare with others. 66MB of updates were also provided. One of the installation steps is the option to run the product as a centrally managed client or as a standalone product. Everything is clear and well described, making for a simple and problem-free set-up. A reboot is needed to complete things.

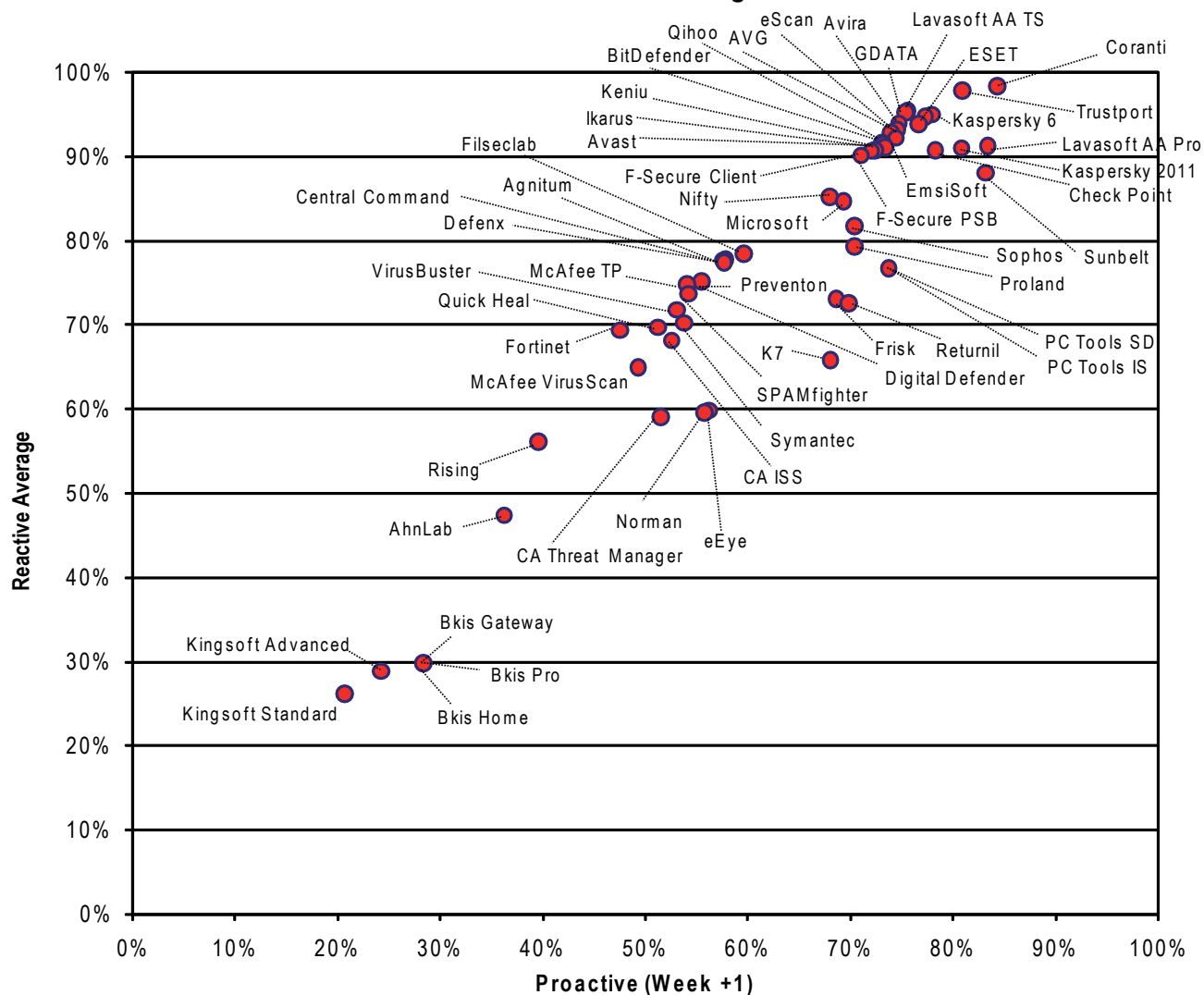
The interface is glossy and slick, with a splendid level of configuration as one might expect from a proper enterprise-grade solution, and everything is easy to find and use. Scanning speeds were not bad on demand, and overheads fairly notable on access, with no sign of the expected caching of good results – much of this work may have been moved into the ‘cloud’. In the resource use tests, memory consumption was perhaps a little above average, but processor use barely registered.

In the infected sets, we noted some rather odd behaviour with a long weekend scan, which seemed to run in fits and starts, spending most of the day on Sunday on only a few files, but clocking up tens of thousands over the following night. Checking through results, we saw the usual pretty solid scores in the main sets. Decent detection levels were displayed in the early RAP sets, declining fairly rapidly in the later weeks; additional detection components not covered by our tests should improve things in real-world use. The WildList set presented no problems, and with no issues in the clean sets either a VB100 is comfortably earned by *Symantec*.

Trustport AntiVirus 2010 5.0.0.4129

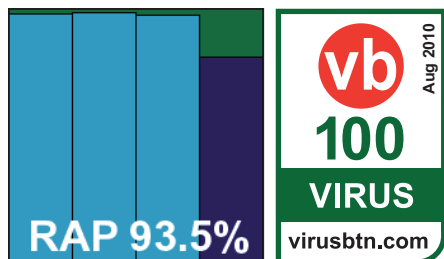
ItW	100.00%	Polymorphic	100.00%
ItW (o/a)	100.00%	Trojans	98.35%
Worms & bots	98.69%	False positives	0

RAP detection scores - August 2010



Trustport's dual-engine approach justifies its above-average 174MB installer, which requires a fairly standard number of

'next' clicks and a reboot to get itself in place. The interface seems mainly designed to be operated via the system tray



menu, but does provide a proper central configuration system with plenty of fine-tuning options. Scanning speeds were somewhat slow, thanks to the dual engine approach, but on access some excellent speed-up was observed in the 'warm' measures, and resource usage was impressively low as well.

Detection rates, as usual, were almost unfailingly splendid, with very little missed anywhere, and with no false alarms to counterbalance the excellent scores. The WildList was swept mercilessly aside, and *Trustport* storms its way to another VB100 award.

VirusBuster Professional 6.2.54

ItW	100.00%	Polymorphic	89.73%
ItW (o/a)	100.00%	Trojans	78.57%
Worms & bots	82.46%	False positives	0

The *VirusBuster* engine has already appeared a phenomenal number of times in this month's comparative.

The company's own version of the scanner came as a 57MB installer with 66MB of updates, and took a fair number of unchallenging steps but no reboot to get in place. The interface itself has also been seen before this month; it is fairly clear in general, if a little fiddly to operate in places, and while its styling may leave something to be desired it remains remarkably solid and well behaved.

Scanning speeds and detection rates alike were solid and decent, if not particularly exceptional, but resource usage seemed surprisingly high compared to others with near-identical set-ups; regrettably no time was available to retest. With no issues in the WildList or clean sets, another solid performance earns *VirusBuster* a clean VB100 award, bringing another epic comparative to a satisfying conclusion.

CONCLUSIONS

Well it has been quite a month. With half of the lab team out of action for much of the month due to serious illness, an epic haul of products to work through and heat building up in the lab thanks to major expansion of the hardware in use, things were never going to be easy. As time went on and more and more products caused problems, it may be that the comments in this month's write-up became less kind than they may usually be. We saw some real howlers this month: some terrible product design, lack of accountability for activities, blatant false alarms in major software, numerous problems detecting the WildList set, but most of all some horrendous instability under pressure.

Some may argue that we put products under stresses they would never be expected to withstand in normal everyday use, but 'flaky' is probably the last word you would want to associate with software meant to keep you safe. If a solution

can be brought to its knees, or worse still, bring an entire system to a standstill simply by having to detect and block the things it is designed to detect and block in higher than usual numbers, many would find it a less than reassuring barrier against attack. We are seriously considering adding some stipulations to the VB100 rules that would disqualify any product which causes a serious crash or which repeatedly ceases to operate.

This month has not had any shortage of failing products, with swathes of false alarms, most of them in software which could not in any way be considered obscure or insignificant, and a larger than usual number of misses in the WildList set too. The WildList is regularly decried as being too limited and easy a selection of samples to use as the basis for certification. This month has made it clear that this is far from a formality, presenting a real challenge to products which ought to be covering the WildList effortlessly from the moment the list is made available. This is not a test of complete in-depth coverage of the entire malware threatscape, merely a measure of regularity, reliability and attention to detail. Perhaps this is a little harsh on those who failed due to problems with W32/Virut samples, as these strains are notoriously complex and difficult to detect, but even here labs should be working hard to make sure they cover all strains impeccably.

The month hasn't been without its happier moments, though, with several newcomers appearing and at least one long-time entrant finally earning its first, much deserved VB100 award. For many, however, this month will hopefully be a salutary lesson that quality cannot be taken for granted but is something that must be worked at constantly. QA departments are one of the most vital parts of any software business, and proper, in-depth internal testing is a must for software aiming to provide reliable, trustworthy protection. We can only hope that this lesson will be taken to heart, and that our next comparative will prove a smoother, less stressful ride.

Technical details:

Test environment: All tests were performed on identical systems with *AMD Phenom II x2 550* processors at 3.11 GHz, 4 GB RAM, and dual 80GB and 1TB *SATA* hard drives, running *Microsoft Windows Vista Business Edition SP2* (x32).

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>.

