AUGUST 2011

virus BULLETIN

Fighting malware and spam

VB100 COMPARATIVE REVIEW ON WINDOWS VISTA X64

INTRODUCTION

This time last year, when we published our previous test on *Windows Vista* (see *VB*, August 2010, p.21), I speculated that it might be the final appearance of the platform in these pages. *Vista* has been plagued by criticisms and complaints since its first appearance in 2007, and has quickly been superseded by a far superior replacement in *Windows 7*, while its supposed predecessor *Windows XP* still refuses to fade away.

Usage of *Vista* has continued to decline very gradually though, with estimates this time last year putting it on around 20% of desktops and the latest guesses ranging from 10% to 15%. This makes it still a pretty significant player in the market, and until those lingering users replace their OS with something better (be it newer or older), we feel obliged to continue checking how well served they are by the current crop of anti-malware solutions. Gluttons for punishment that we are, we opted to try a 64-bit version of the platform, which seemed almost guaranteed to bring out any lingering shakiness in products, many of which have proven themselves in recent tests to be highly susceptible to collapsing under any sort of pressure.

PLATFORM AND TEST SETS

Preparing the test systems in something of a hurry after several recent tests overran, we found the set-up process to be rather more painful than usual, mainly thanks to the need to apply two service packs separately from the media to hand. With this done, and the resulting clutter mopped up, we made the usual minor tweaks to the systems, installing a handful of useful tools, setting up the networking and desktop to our liking and so on, before taking snapshots of the systems and moving on to preparing the sample sets.

The clean set saw a fair bit of attention this month, with the usual cleanup of older and less relevant items, and the addition of a swathe of new files culled from magazine cover CDs, the most popular items from major download sites, as well as items from the download areas of some leading software brands. After dumping a fair amount of older clutter, the final set weighed in at just over half a million files, 140GB.

Building the sets of malicious samples using all new files seen during the appropriate periods – June for the RAP set and May for the sets of trojans, worms and bots – led to some rather large collections in each category, which needed verification and classification to bring them down to a manageable size. Initial tests were run with the unfiltered sets, but these were trimmed down in time for the products which we expected to be troublesome, with further filtering continuing throughout the test period. Final numbers were around 35,000 samples in the worms and bots set; 120,000 trojans; and an average 40,000 for each of the weekly RAP sets.

The clean sample sets used for the speed measures remained unchanged. The speed test scripts were adjusted slightly to include more runs of the collection of standard activities – this test was run ten times per product this month, with the average time to complete the jobs compared with a baseline figure taken from multiple runs on clean systems.

The WildList set included nothing too remarkable, with several more variants of W32/Virut falling off the list, leaving very few complex polymorphic items remaining. As testing drew to a close, the *WildList Organization* made public its new extended list, with a wider range of malware types included – we plan to include this as part of our requirements for future tests, more on which later.

With everything set up and ready to go, it was time to start working through this month's list of products, all submitted by the deadline of 22 June. The final list totalled 48 products – a number which a couple of years ago would have been

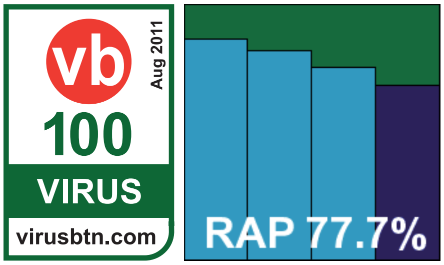
ISSN 1749-7027

a record, but compared to some recent tests actually seems rather small. To get through the work in reasonable time, we opted to keep to our plan introduced last time, of capping speed measures at two hours to prevent slowpokes taking up too much of our precious time; we also decided to keep a closer eye on just how long each product took to complete the full suite of tests and explicitly report it, along with details of any crashes, hangs or other problems which caused us headaches. Of course, as some of the tests involve unrealistic scenarios – such as intensive bombardment with infected samples – slow completion times and bugs are not considered in themselves cause to deny a product certification, but they may be of some interest to our readers.

Agnitum Outpost Security Suite Pro 7.1

Version 3415.520.1248, Anti-Malware database 22/06/2011

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.34%
Worms & bots	92.31%	**False positives**	0



First up on this month's product roster, *Agnitum* has a solid record in our tests but has been causing some unexpected slowdowns of late. The 101MB install package ran through its process fairly slowly thanks to a large number of stages, including an option to join a community scheme disguised as a standard EULA acceptance. When the set-up was eventually complete, and following the required reboot, speed tests ran through without issues, but took quite some time. There were heavy lag times accessing files, slow scanning speeds, and a hefty impact on our activities suite. CPU use was also high, although RAM use was not excessive.

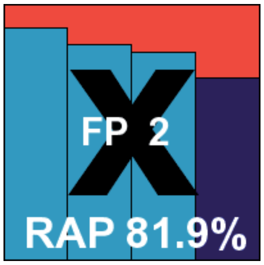
Getting through the clean set took an outrageously long time – over 58 hours. We later noted that the fastest time for a product to complete this task this month was less than an hour. Given that these are clean files only, it seems unlikely that any real-world user would be prepared to countenance such sluggish scanning speeds. By comparison, the malware sets were processed in quite reasonable time, adding only another day to the total testing time. Detection rates were pretty solid as usual, with respectable scores in the main sets and decent levels in the RAP sets, declining steadily but not catastrophically through the four weeks.

The core requirements in the WildList and clean sets were met without problems, and *Agnitum* earns another VB100 award. This gives the vendor five passes and one no-entry in the last six tests; eight passes and four no-entries in the last two years. This month's test showed no crashes or other problems, but the slowdowns meant that testing – which we had hoped to complete within 24 hours – took more than five full days to get through.

AhnLab Internet Security 8.0

Product version 8.0.4.7 (Build 940), Engine version 2011.06.21.90

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	96.11%
Worms & bots	96.64%	**False positives**	2



AhnLab's current product arrived as a fairly large 180MB install package, although no further updates were required, and the set-up process was speedy and simple, completing in a handful of clicks and a minute or so of waiting, with no need to reboot. On completion however, *Windows* popped up a dialog suggesting that the product hadn't installed correctly, although all seemed to be in order.

The interface is clean and neat, and a good level of configuration is available for the numerous components, without too much difficulty navigating – although in some places controls are not grouped quite as one might expect. Scanning speeds were fairly slow, especially in the set of executable files, and on-access lag times were also fairly heavy; CPU use was very high when the system was busy, but RAM use was low and impact on our suite of tasks was not too intrusive either.

The detection tests were hampered by blue screens during the intensive on-access tests, with errors warning of page faults in non-paged areas. We also had problems with the on-demand tests, with logs reporting larger numbers of items found than were displayed in the log viewer utility. After several attempts we managed to get a complete set of data together, showing some pretty good detection rates, with high scores in the main sets and a good level in the RAP sets, declining steadily into the proactive week. The WildList was handled well, but in the clean sets a couple of items, including the popular *Thunderbird* mail client, were labelled as malware, denying *AhnLab* a VB100 award this month.

On-demand detection	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2859	92.31%	0	100.00%	8293	93.34%		
AhnLab IS	0	100.00%	1248	96.64%	4	99.99%	4843	96.11%	2	
Avast Software avast!	0	100.00%	223	99.40%	1	99.99%	1327	98.93%		
AVG Internet Security	0	100.00%	640	98.28%	4	99.99%	3077	97.53%	2	
Avira AntiVir Pers.	0	100.00%	294	99.21%	0	100.00%	2170	98.26%		
Avira AntiVir Pro.	0	100.00%	294	99.21%	0	100.00%	2170	98.26%		
BitDefender Security	0	100.00%	316	99.15%	0	100.00%	4389	96.47%		
BullGuard Antivirus	0	100.00%	144	99.61%	0	100.00%	618	99.50%		
Central Command Vexira	0	100.00%	2871	92.28%	0	100.00%	8487	93.18%		
Clearsight Antivirus	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%		
Commtouch Command	0	100.00%	9221	75.21%	0	100.00%	24368	80.42%		
Comodo Antivirus	0	100.00%	740	98.01%	418	95.51%	5592	95.51%	4	11
Comodo IS PREMIUM	0	100.00%	740	98.01%	418	95.51%	5592	95.51%	4	11
Defenx Security Suite	0	100.00%	2928	92.13%	30	99.92%	8744	92.97%		
Digital Defender	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%		
eEye DS Blink	0	100.00%	2535	93.18%	4	99.98%	7227	94.19%	6	6
Emsisoft Anti-Malware	0	100.00%	207	99.44%	436	95.80%	482	99.61%	2	2
eScan IS Suite	0	100.00%	141	99.62%	0	100.00%	647	99.48%		
ESET NOD32 Antivirus	0	100.00%	1227	96.70%	0	100.00%	5770	95.36%		21
Fortinet FortiClient	0	100.00%	969	97.39%	0	100.00%	2648	97.87%		
Frisk F-PROT	0	100.00%	9569	74.27%	0	100.00%	25975	79.13%		
F-Secure Client Security	0	100.00%	183	99.51%	0	100.00%	4012	96.78%		
G Data AntiVirus	0	100.00%	29	99.92%	0	100.00%	210	99.83%		
GFI VIPRE Antivirus	0	100.00%	1025	97.24%	19	99.80%	3800	96.95%		

(Please refer to text for full product names)

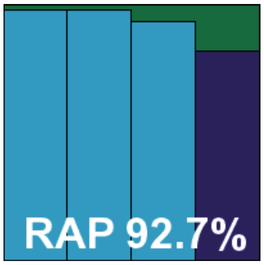
The vendor's record has been somewhat patchy of late, with two passes, two fails and two tests not entered in the last six. Over the last two years *AhnLab* has had five passes, four fails and three missed tests. This month testing took five full days to complete, with the main problems being blue screens causing a total system crash twice during heavy bombardment, the on-access component falling over occasionally, and issues with the logging system.

Avast Software avast! Free Antivirus 6

Program version 6.0.01184, Virus definitions version 110622-1

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	98.93%
Worms & bots	99.40%	**False positives**	0

vb
Aug 2011
100
VIRUS
virusbtn.com



Avast's version 6 came hot on the heels of version 5, and is pretty similar in many respects, the main addition being a sandboxing system for suspect items. The installer is compact at 58MB including all updates, and runs through rapidly with minimal input required from the user; the main item of note is the offer to install the *Google Chrome* browser, a fairly typical add-on with free software but not something which pleases everyone. No reboot was needed to complete the set-up process.

The interface remains very easy on the eye and a pleasure to use, with a splendid depth of configuration provided for advanced users without making things seem too complicated for novices. The control system features detailed explanations throughout to allow less knowledgeable users to make informed decisions about how things should run, avoiding the jargon-heavy approach of some lazier developers.

Scanning speeds were blisteringly fast as always, powering through the sets in excellent time with a light touch when accessing files (perhaps helped somewhat by the default approach of not scanning all file types on-read). Resource use was pretty low, with very little impact on our set of activities.

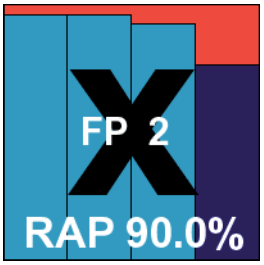
Scores were excellent, with splendid coverage of all our sets, a small drop notable in the proactive portion of the RAP sets but still highly impressive even there. The clean set, which some products plodded through in days, was brushed aside in record time, and the infected sets handled rapidly and accurately too; no problems were encountered in the certification sets, earning *Avast* another VB100 award, the vendor's 16th consecutive pass.

All tests completed in well under the 24 hours we hoped all products would manage, with no issues at all, making for an all-round excellent performance.

AVG Internet Security Business Edition 2011

AVG version 10.0.1382, Virus DB 1513/3719

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	97.53%
Worms & bots	98.28%	**False positives**	2



While fellow Czech company and arch rival *Avast* routinely submits its free edition for our tests, *AVG* tends to enter its full premium suite solutions, with this month's entry being the corporate desktop product. The installer is a fair size at 183MB, with all updates included, and runs through in short order with a half-dozen clicks of 'next' and no need to reboot, despite the multiple layers of protection included. Part of the process is the offer of a browser security toolbar, use of a secure search facility, and a groovy Aero sidebar gadget.

The interface is clear and simply laid out, with a sober grey colour scheme suitable for business users. Under the hood is another excellent set of fine-tuning controls, again provided in splendid depth and made reasonably clear and simple to operate even for untrained users. It remained responsive and stable throughout testing.

Speed measures were decent to start with, and sped up hugely in the warm measures, both on demand and on access. Resource use was low, as was impact on our set of tasks. Getting through the larger test sets took a little time but wasn't excessively slow, and the infected sets were handled excellently, with highly impressive scores in the main sets and the reactive parts of the RAP sets, dropping a little in the proactive week.

The WildList was handled well, but in the clean sets a couple of items were mislabelled as malware, including part of a photo manipulation suite from Canadian developer *Corel*, which seems to produce regular issues in our testing. Both alerts were only heuristic detections, but this was enough to deny *AVG* a VB100 award this month, spoiling a solid record of passes dating back to 2007.

On-demand detection contd.	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Ikarus virus.utilities	0	100.00%	258	99.31%	436	95.80%	542	99.56%	2	2
Iolo System Shield	0	100.00%	11053	70.28%	0	100.00%	33053	73.44%		
Kaspersky IS 2012	0	100.00%	2291	93.84%	0	100.00%	5548	95.54%		
Kaspersky SO Security 2	0	100.00%	2290	93.84%	0	100.00%	5538	95.55%	1	
Lavasoft Ad-Aware TS	0	100.00%	212	99.43%	0	100.00%	4058	96.74%		
LogicOcean Gprotect	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%		
McAfee VirusScan	0	100.00%	2066	94.44%	0	100.00%	4600	96.30%		
Microsoft SE	0	100.00%	1629	95.62%	0	100.00%	11677	90.62%		
Norman Security Suite	0	100.00%	2531	93.19%	4	99.98%	7188	94.22%	3	2
PC Booster AV Booster	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%		
PC Tools Internet Security	0	100.00%	1343	96.39%	0	100.00%	6573	94.72%	16	
PC Tools SD with AntiVirus	0	100.00%	1343	96.39%	0	100.00%	6574	94.72%	16	
Preventon	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%		
Qihoo 360 Antivirus	0	100.00%	134	99.64%	0	100.00%	540	99.57%		
Quick Heal Antivirus Pro	0	100.00%	3434	90.77%	0	100.00%	12453	89.99%		
Returnil System Safe	0	100.00%	9229	75.18%	0	100.00%	24388	80.40%		
Rising Internet Security	0	100.00%	28045	24.59%	20	99.95%	82677	33.56%		156
Security Coverage SecureIT	0	100.00%	428	98.85%	0	100.00%	2233	98.21%		
Sophos ESC	0	100.00%	1715	95.39%	0	100.00%	8011	93.56%		
SPAMfighter VIRUSfighter	0	100.00%	3233	91.31%	0	100.00%	13298	89.31%		
Total Defense ISS Plus	0	100.00%	4395	88.18%	4	99.96%	17543	85.90%		
Total Defense TD r12	0	100.00%	5856	84.25%	160	99.33%	33863	72.79%		
TrustPort Antivirus 2012	0	100.00%	37	99.90%	0	100.00%	119	99.90%		
VirusBuster Professional	0	100.00%	2868	92.29%	0	100.00%	8489	93.18%		

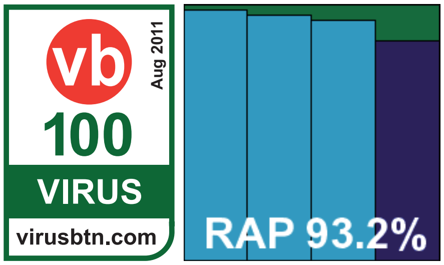
(Please refer to text for full product names)

This result now brings the vendor to five passes and a single fail in the past year; ten passes, one fail and one test not entered in the last 12. The product completed the full set of tests this month in around 24 hours, our target time, and there were no issues other than the two false positives in the clean sets.

Avira AntiVir Personal

Product version 10.0.0.648, Virus definition file 7.11.10.48

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.26%
Worms & bots	99.21%	**False positives**	0



Avira's free edition has become a regular in our tests in the last few years, and is generally a welcome sight. The installer is small at 51MB, but an additional 44MB update package is also provided. Getting set up is fairly simple, with another half-dozen dialogs offering the usual information and options, with good clarity, and a speedy install with no need to reboot. The only item of note is the rather large advertising screen pushing the paid-for edition, which comes at the end of the process.

The product interface is a little less slick than some, with a rather sparse, angular look to it, and the minimal language marking controls and options is occasionally less than clear. Nevertheless, once again an excellent level of controls is provided, with simple and expert modes to protect the less advanced user from the more frightening technical stuff.

Scanning speeds were decent, improving very slightly in the warm runs but not enough to make a huge impact, while on-access overheads were in the mid-range. Resource consumption was excellent, with very little RAM or CPU used and minimal effect on our set of activities.

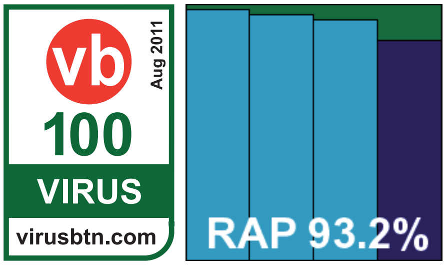
The rest of the tests were powered through in splendid time, with no issues, recording a clean run through the false positive sets and splendid detection rates in all the infected sets, dipping only very slightly towards the end of the RAP sets. The WildList caused no issues, easily earning *Avira* another VB100 award for its free edition.

This version has yet to hit a single snag, with three passes from three attempts in the last six tests, five passes from five attempts in the last two years. Tests completed comfortably within the 24-hour time frame, with no sign of any instability or other problems.

Avira AntiVir Professional

Product version 10.0.0.1012, Virus definition file 7.11.10.48

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.26%
Worms & bots	99.21%	**False positives**	0



Weighing in a fraction heavier than the free edition at 58MB, and using the same 44MB update package, *Avira*'s premium version is pretty similar in a lot of ways, the simple and speedy install process following similar lines and finishing just as rapidly, with again no need to restart. The interface has a very similar look and feel, with again an excellent level of controls tucked away in the 'Expert mode' area.

Tests zipped through in good time – the on-demand speeds were noticeably quicker than those shown by the free version, but the on-access measures were hard to tell apart. Use of memory was just as low as the free edition, but CPU use was slightly increased and impact on our set of tasks also a little higher.

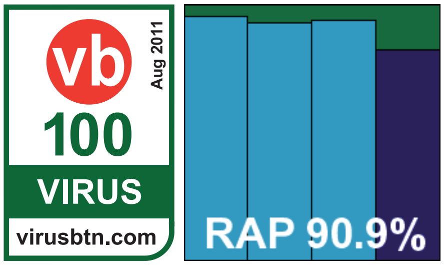
Detection rates were identical though, showing that the free version is in no way the lesser. Here again we saw superb coverage of our infected sets, including complete detection of the WildList set, and with no issues in the clean sets another VB100 award is comfortably earned by *Avira*.

This pro version has a rather longer history in our tests than the free one, and maintains an excellent record, with all of the last six tests passed; a single fail and 11 passes in the last two years. *Avira*'s popularity with the lab team is strengthened by another easy test month, all tests completing in under a day with no sign of any problems anywhere.

BitDefender Security for File Servers

Product version 3.5.17.1, Antivirus signatures 8348918

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.47%
Worms & bots	99.15%	**False positives**	0



Somewhat surprisingly, *BitDefender* submitted its file server edition for this month's comparative, but since we had seen the same solution in the previous test it presented few problems. The installer was fairly large at 186MB, including updates, but the set-up process is fairly standard with no surprises and ran through quickly, with no reboot needed to complete.

The interface is based on the MMC system, but is more colourful and easy to operate than many similar systems, with plenty of control options (as one would expect from a server-level product). Scanning speeds were middle of the road, with no sign of any speed-up in the warm measures, but some form of caching was clearly present in the on-access mode, which is where it really counts. Overheads were not too heavy to start with, and barely noticeable once files had passed initial checks.

In everyday use, consumption of memory was fairly low, but CPU use was noticeably high, and our suite of standard tasks took a little longer to complete than expected. The on-access detection measures ran through in decent time, with solid stability even under heavy bombardment, but in the on-demand jobs things got a little trickier. We have noticed several products of late storing scan results in memory until the end of the job, only writing to disk once complete (or, in some cases, once the user has acknowledged completion). This is presumably an optimization measure, but seems rather unnecessary – assuming a scan detects little or nothing, as should be the norm, the time spent writing out to file would be minute, whereas when multiple detections occur (the only situation in which such optimization would help), the escalating use of RAM can cause all sorts of problems.

BitDefender's developers have clearly not thought this through, and have not implemented any sort of checking of how much memory is being eaten up by the product – the scan of our main sets slowly stumbled to a crawl as system resources were drained. Day after day passed, with the team leaving the lab each evening vainly hoping that the scan would be finished in the morning. By the fifth day (the fastest time taken to complete this job this month was less than two hours), almost 2GB of RAM was being used by the scanning process, and the machine was barely responsive. At this point, a power outage hit the test lab thanks to a UPS failure, and a whole week's worth of work was lost forever, thanks to the product's failure to back things up to the hard disk.

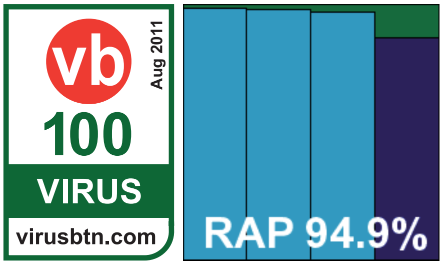
Re-running the tests in smaller chunks proved a much faster approach, as the lack of excessive memory use kept things ticking over nicely, but of course it required much more hands-on work from the lab team. Eventually, we gathered a full set of results from over 20 scans, and they showed the usual excellent scores. All sets were well covered, with some stellar figures in the RAP sets, only declining slightly in the proactive week. The core requirements were comfortably met and a VB100 award is duly earned after some considerable hard work from us.

BitDefender's record is solid, with all of the last six tests passed, and ten passes, one fail and one no-entry in the last two years. There were no actual crashes in this month's test, and the slowdown we saw due to heavy RAM use would only occur in extreme circumstances. Nevertheless, testing took up more than eight full days of lab time.

BullGuard Antivirus 10

BullGuard version 10,0,0,26, BpAntivirus version 10,0,0,48

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.50%
Worms & bots	99.61%	**False positives**	0



BullGuard's solution is based around the same engine as *BitDefender*, and the installer is again fairly large at 155MB. The set-up process involves only a few clicks, but takes a little time to run through, needing no reboot to finish off. The interface is a little quirky, but fairly usable after a little exploration, and operated fairly stably throughout testing, although we did notice some lengthy pauses when opening saved scan logs.

Speed measures were pretty fast, with caching implemented in both on-demand and on-access modes, and RAM and CPU use were around average, while impact on our set of tasks was again a little higher than most. Running through the detection tests proved fairly painless, with no problems getting through large scans, and the on-access measures completed in good time too, although we did note that some sort of lockdown was imposed when large numbers of detections were bombarding the protection system, resulting in many other activities being prevented.

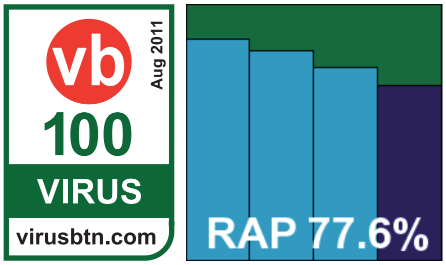
Scores were excellent throughout the sets, with even the proactive week of the RAP sets very well covered. The WildList set and clean sets threw up no surprises, and *BullGuard* comfortably earns another VB100 award. It now has four passes and two no-entries in the last six tests; six passes and six no-entries in the last two years. There were no serious stability problems during testing, which completed in around the 24 hours allotted to each product.

Central Command Vexira Antivirus Professional

Version 7.1.70, Virus scan engine 5.3.0, Virus database 14.0.91

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.18%
Worms & bots	92.28%	**False positives**	0

Central Command's product is now a regular participant in our tests. The current version of the product was submitted as a 68MB installer with a 59MB update bundle, which ran through in quite a few steps, taking some time. Like others based on the *VirusBuster* engine of late, the permission to join a community feedback scheme was sneakily concealed where the 'accept' option for the EULA would usually be found. The slowish process ends with a reboot.



The product interface is highly reminiscent of those seen in *VirusBuster* products for many years now, but in a garish red. The layout remains fiddly and awkward, lacking more than a little in intuitiveness, but provides a reasonable degree of control. Scanning speeds were fairly decent, but on-access overheads seemed a little above average in some areas, while use of resources and impact on our set of tasks were also higher than many this month, although not outrageously so.

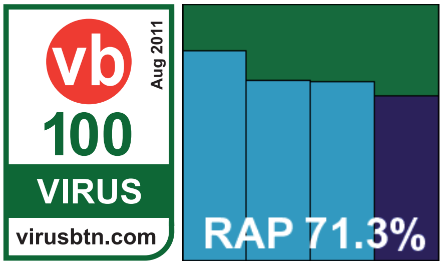
Detection rates were decent in the main sets and reasonable in the RAP sets, tailing off slightly through the weeks. The core certification sets were handled well, and *Central Command* earns another VB100 award without too much strain. The vendor's record shows an impeccable nine passes from nine entries since re-emerging in its current form; tests ran smoothly with no problems, and completed within 24 hours.

Clearsight Antivirus

Version 1.1.68, Definitions version 14.0.90

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.61%
Worms & bots	91.69%	**False positives**	0

As usual this month's test sees a number of very similar products based on the popular *VirusBuster* engine, using an SDK developed by *Preventon*. First up is *Clearsight*, which already has a handful of successful VB100 entries under its belt. The installer is a fairly compact 63MB, including all the latest updates, and runs through swiftly and simply, although it does complain if Internet connectivity is not available at install time. We left the system connected long enough to apply a licence key (needed to access full configuration controls), but blocked any updating past the deadline date. No reboot is needed to complete the set-up.



The interface is simple and hard to get lost in, providing basic controls covering a reasonable range of fine-tuning with minimal fuss. Operation proved smooth and stable, with no issues even under heavy pressure, and testing completed without incident. Scanning speeds were not the fastest, but still pretty decent and very consistent over multiple runs, while on-access overheads and resource consumption measures were similarly middling, with a small but noticeable impact on our suite of tasks.

Detection rates were decent – no threat to the leaders of the pack but far from the tail too – with a steady but not too steep decline through the RAP sets. The WildList and clean sets were handled properly, earning *Clearsight* another VB100 pass – its third in a row with a single fail and one no-entry since its first appearance five tests ago. Testing ran through without incident, taking just a little longer than the expected full day to complete.

Commtouch Command Anti-Malware

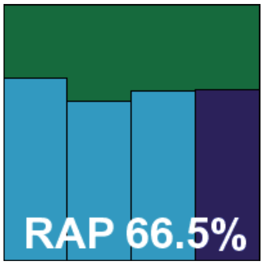
Product version 5.1.14, Engine version 5.3.5, DAT file ID 201106220548

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	80.42%
Worms & bots	75.21%	**False positives**	0

On-access detection	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	3046	91.81%	0	100.00%	12137	90.25%
AhnLab Internet Security	0	100.00%	1492	95.99%	90	99.87%	5573	95.52%
Avast Software avast! Free Antivirus	0	100.00%	230	99.38%	1	99.99%	1513	98.78%
AVG Internet Security	0	100.00%	793	97.87%	4	99.99%	4370	96.49%
Avira AntiVir Personal	0	100.00%	368	99.01%	0	100.00%	2800	97.75%
Avira AntiVir Professional	0	100.00%	368	99.01%	0	100.00%	2800	97.75%
BitDefender Security for File Servers	0	100.00%	145	99.61%	0	100.00%	595	99.52%
BullGuard Antivirus	0	100.00%	274	99.26%	0	100.00%	1255	98.99%
Central Command Vexira	0	100.00%	3053	91.79%	0	100.00%	12373	90.06%
Clearsight Antivirus	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%
Commtouch Command Anti-Malware	0	100.00%	9550	74.32%	0	100.00%	25999	79.11%
Comodo Antivirus	0	100.00%	925	97.51%	418	95.51%	6933	94.43%
Comodo Internet Security PREMIUM	0	100.00%	925	97.51%	418	95.51%	6933	94.43%
Defenx Security Suite 2011	0	100.00%	3046	91.81%	0	100.00%	12137	90.25%
Digital Defender Antivirus Pro	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%
eEye Digital Security Blink Professional	0	100.00%	2718	92.69%	38	99.68%	8189	93.42%
Emsisoft Anti-Malware	0	100.00%	NA	NA	NA	NA	NA	NA
eScan Internet Security Suite	0	100.00%	302	99.19%	0	100.00%	4267	96.57%
ESET NOD32 Antivirus	0	100.00%	2401	93.54%	0	100.00%	17561	85.89%
Fortinet FortiClient	0	100.00%	969	97.39%	0	100.00%	2648	97.87%
Frisk F-PROT Antivirus for Windows	0	100.00%	9792	73.67%	0	100.00%	28810	76.85%
F-Secure Client Security	0	100.00%	228	99.39%	0	100.00%	3560	97.14%
G Data AntiVirus 2012	0	100.00%	30	99.92%	0	100.00%	97	99.92%
GFI VIPRE Antivirus	0	100.00%	2497	93.29%	38	99.52%	4522	96.37%

(Please refer to text for full product names)

vb
Aug 2011
100
VIRUS
virusbtn.com



We have grown quite used to the *Commtouch* name by now, although the product's pre-acquisition company name, *Authentium*, still crops up from time to time in team discussions. This is also the case in the product itself, with the installer, a tiny 14MB with an additional 28MB update bundle, dropping a few files and folders still referencing the old brand as part of its speedy, low-interaction set-up process. With no reboot needed even after the updates were applied using a custom script, things were ready to go in only a minute or so.

Operation is fairly straightforward, with a fairly basic set of options available once the button to enable the 'advanced' mode has been clicked. Scanning speeds were not super fast, with on-access overheads a little higher than many this month, and while RAM use was not exceptional, both CPU use and impact on our set of activities were pretty high.

Detection rates were unspectacular, with a reasonable showing in the main sets and respectable, surprisingly consistent scores in the RAP sets. The WildList brought no surprises, and with only a handful of suspicious files in the clean sets – alerting on suspicious packing practices and adware – *Commtouch* has no problems earning a VB100 award this month.

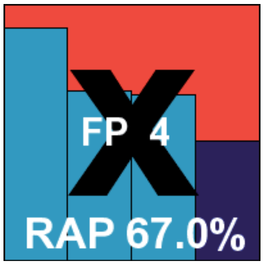
Our records for the product show a somewhat patchy history lately, with three passes and two fails from five entries in the last six tests; four passes, four fails and four tests not entered in the last two years. A single minor issue was observed during testing, when a large log file failed to fully export properly, but the problem did not recur and testing completed just within the 24 hours allotted to the product.

Comodo Antivirus

Product version 5.4.191918.1356, Virus signature database version 9154

ItW	100.00%	**Polymorphic**	95.51%
ItW (o/a)	100.00%	**Trojans**	95.51%
Worms & bots	98.01%	**False positives**	4

Comodo is a relative newcomer to our tests, having taken part fairly regularly during the last year. The vendor usually submits both the plain *Antivirus* edition alongside the full suite. The two products are pretty similar, even down to using the same 60MB installer; the difference only takes effect during install, when the user can select the option to include the suite's extra components. Installation was run on the deadline day, starting with a wide selection of available languages, some of which are provided by the product's 'community' of fans. Alongside the usual install steps is an option to use *Comodo*'s own secure DNS servers, and with a reboot to complete, this first step took only a minute or two to get through. On restart, the product goes online to fetch updates, which in this case took 15 to 20 minutes to fetch 122MB of data.



The product is pretty good looking, with clean and elegant lines and a crisp red-and-deep-grey colour scheme. The layout follows a common pattern, making it simple to navigate, and provides a lot of extras alongside the usual basics of anti-virus, including the 'Defense+' intrusion prevention system and sandboxing of unknown executables. A good level of controls are provided, with plenty of clear and useful explanation.

Running the first tests was thus simple and rapid, with some fairly fast scanning speeds and on-access overheads medium in some areas and light in others. Resource use was also medium, although impact on our set of tasks was a little high.

Running the larger tests took quite some time though, despite following advice from the submitters to disable cloud look-ups. The on-access run over our main sets took nine full days, and the scan of our clean sets, RAP and main infected sets took considerably longer. Throughout this period the machine remained stable and responsive, with no sign of any other problems, and the slowness is likely only to affect scans of large amounts of infected items – an unlikely scenario in the real world.

With the results finally in, we saw some pretty decent detection rates in the main sets, with the RAP sets starting off pretty good too, but dropping very sharply through the weeks to a rather poor level in the proactive week – implying that detection of more recent items leaves something to be desired. The WildList was handled well, and in the clean sets a number of items were warned about, including any file with more than one extension being alerted on as 'Heur.Dual.Extension' – probably a wise move given the ongoing use of such tricks to disguise malware. Several other items were described as 'Suspicious', while a few full-blown false positives were also recorded, including the popular *FileZilla* downloading tool being flagged as a downloader trojan.

On-access detection contd.	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Ikarus virus.utilities	0	100.00%	258	99.31%	436	95.80%	542	99.56%
Iolo System Shield	0	100.00%	9559	74.30%	0	100.00%	26098	79.03%
Kaspersky Internet Security 2012	0	100.00%	2401	93.54%	0	100.00%	6455	94.81%
Kaspersky Small Office Security 2	0	100.00%	2387	93.58%	0	100.00%	6370	94.88%
Lavasoft Ad-Aware Total Security	0	100.00%	97	99.74%	0	100.00%	1324	98.94%
LogicOcean Gprotect	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%
McAfee VirusScan Enterprise	0	100.00%	2120	94.30%	6	99.99%	4908	96.06%
Microsoft Security Essentials	0	100.00%	2208	94.06%	0	100.00%	13484	89.16%
Norman Security Suite	0	100.00%	2685	92.78%	38	99.68%	8142	93.46%
PC Booster AV Booster	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%
PC Tools Internet Security	0	100.00%	2170	94.17%	0	100.00%	8179	93.43%
PC Tools Spyware Doctor with AntiVirus	0	100.00%	1677	95.49%	0	100.00%	7624	93.87%
Preventon	0	100.00%	3091	91.69%	0	100.00%	12933	89.61%
Qihoo 360 Antivirus	0	100.00%	321	99.14%	0	100.00%	4554	96.34%
Quick Heal Antivirus Pro 2011	0	100.00%	8169	78.04%	0	100.00%	34393	72.36%
Returnil System Safe	0	100.00%	9779	73.71%	0	100.00%	28724	76.92%
Rising Internet Security	0	100.00%	27816	25.21%	414	99.33%	78314	37.06%
Security Coverage SecureIT 2011	0	100.00%	144	99.61%	0	100.00%	613	99.51%
Sophos Endpoint Security and Control	0	100.00%	1113	97.01%	0	100.00%	6901	94.45%
SPAMfighter VIRUSfighter	0	100.00%	3233	91.31%	0	100.00%	13303	89.31%
Total Defense Inc. Internet Security Suite Plus	0	100.00%	4501	87.90%	4	99.99%	18859	84.84%
Total Defense Inc. Total Defense r12	0	100.00%	6998	81.18%	4	99.99%	20121	83.83%
TrustPort Antivirus 2012	0	100.00%	115	99.69%	0	100.00%	1395	98.88%
VirusBuster Professional	0	100.00%	3053	91.79%	0	100.00%	12373	90.06%

(Please refer to text for full product names)

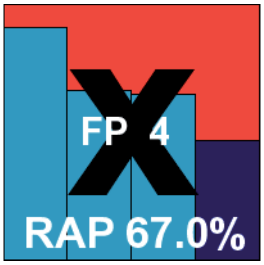
This was enough to deny *Comodo* a VB100 award this month.

The records of the *Antivirus* product show no passes from two previous entries in the last year (the only test *Comodo* has managed to pass so far was the April 2011 *XP* test, which featured the vendor's suite edition). There were no stability problems or crashes during testing, but the slow speed over infected items meant the product hogged one of our test systems for a truly epic 20 days.

Comodo Internet Security PREMIUM

Product version 5.4.191918.1356, Virus signature database version 9154

ItW	100.00%	**Polymorphic**	95.51%
ItW (o/a)	100.00%	**Trojans**	95.51%
Worms & bots	98.01%	**False positives**	4



Comodo's second product this month is the full 'Premium' suite, but as far as we could tell it appears to be available free of charge. Using the same installer as the previous product, the experience was unsurprisingly similar, although in this instance we opted to check both the suite and 'Geek Buddy' options – the latter being a support system allowing engineers to access the local system to fix problems. After the few minutes of installing and a required reboot, the update once again ran for around 20 minutes, downloading the 122MB of data for the main product (we chose not to update the Geek Buddy component, having observed this taking quite some time in previous tests).

With the product set up and an image taken for testing, there was little difference between this and the previous product; the most obvious thing is that this version includes a firewall, but otherwise the interface and operation was identical – clear and easy to use with a good range of components and well laid out controls.

The results of the performance tests were decent – better than average in most areas, with average use of resources and, somewhat oddly, a much lower impact on our set of activities than the product's counterpart. Again the main tests took forever to complete, showing no signs of instability or unresponsiveness but just dawdling enormously. Results showed a similar pattern, with good detection rates in the older areas but considerably lower over more recent items, and although the WildList was fully detected, the same crop of false alarms that tripped up the *Antivirus* version also deny this product a VB100 award.

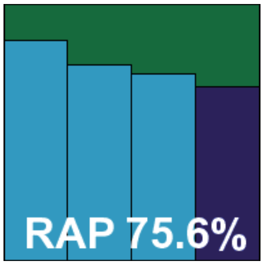
The suite's history is a little better, with one pass and now three fails in the last year, with two tests not entered. There were no crashes, but the slow scanning meant the product also took more than 20 days to get through our tests; between them, *Comodo*'s two solutions took up enough machine time to process 40 products operating at the expected pace – almost the whole of the rest of this month's field.

Defenx Security Suite 2011

Version 2011 (3390.519.1248)

ItW	100.00%	**Polymorphic**	99.92%
ItW (o/a)	100.00%	**Trojans**	92.97%
Worms & bots	92.13%	**False positives**	0

vb 100 VIRUS virusbtn.com Aug 2011



Swiss firm *Defenx* is another relative newcomer which has started to become a regular sight on our test bench over the last few years, with a strong record of passes. Of late we have noted some increasing slowness in our tests, with both malware and speed tests taking a long time to complete; we hoped for a return to previous speeds this month.

The installer weighed in at just under 100MB, and after a few standard stages, including the trick of hiding the option to join a feedback scheme alongside the EULA acceptance (which currently seems standard for products based on the *VirusBuster* engine), it ran through its set-up tasks in a few minutes, with a reboot to finish off.

The interface is very similar to that of the *Agnitum* product, of which this is a spin-off of sorts, and thus devotes much attention to the firewall components in its design – but it still makes some space for the anti-malware module, providing a basic range of controls. Scanning speeds were not fast to start with, with one scan, covering our set of executables, just hitting the two-hour cut-off limit imposed on these measures; in repeat runs things were much quicker. On-access overheads were very heavy though, and bizarrely actually got slower in the warm measures. Use of RAM was a little high, but CPU cycles went through the roof, with a hefty impact on our set of tasks too.

The slowness worsened in the larger detection tests, with the on-access test taking over 20 hours to get through, and

On-demand throughput (MB/s)	System drive*	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	9.38	1.92	1.90	1.92	20.19	20.11	20.19	10.06	20.87	20.61	9.33	9.49	9.33
AhnLab IS	12.60	7.36	7.43	7.36	4.00	4.04	4.00	11.24	23.80	23.02	7.62	7.90	7.62
Avast Software avast!	38.64	126.39	138.43	8.73	34.94	36.49	16.10	18.64	45.61	34.21	18.34	22.54	15.24
AVG Internet Security	40.24	6.13	2906.94	6.13	26.48	1642.04	26.48	13.74	615.76	28.15	9.41	216.40	9.41
Avira AntiVir Pers.	29.41	5.43	5.50	5.27	32.84	34.21	34.21	13.00	32.41	33.28	14.43	16.39	16.91
Avira AntiVir Pro.	29.90	5.92	5.90	5.53	50.78	57.95	57.28	20.73	57.95	49.76	13.04	13.87	13.70
BitDefender Security	25.63	5.17	5.18	5.16	31.38	31.18	31.18	15.72	32.84	33.06	15.46	15.91	15.68
BullGuard Antivirus	14.98	10.85	2906.94	10.69	16.05	4926.11	14.62	6.85	1642.04	14.03	14.43	541.00	14.43
Central Command Vexira	40.03	12.75	12.75	1.41	23.13	23.80	4.47	22.68	49.26	15.94	15.68	16.15	5.49
Clearsight Antivirus	23.43	4.84	4.79	4.84	18.04	19.17	18.04	11.73	24.15	24.03	11.89	12.02	11.89
Commtouch Command	23.24	7.51	8.12	7.51	18.18	18.38	18.18	12.14	25.26	24.88	14.24	14.43	14.24
Comodo Antivirus	9.35	5.01	5.14	5.01	22.81	23.91	22.81	24.05	56.62	49.26	11.89	12.30	11.89
Comodo IS PREMIUM	9.46	5.22	5.51	5.22	23.46	24.51	23.46	23.81	50.78	48.77	11.63	11.63	11.63
Defenx Security Suite	8.00	5.31	88.09	5.31	0.68	18.95	0.68	9.39	19.78	19.24	9.02	9.09	9.02
Digital Defender	23.43	4.80	4.77	4.80	18.31	18.31	18.31	12.08	25.01	24.75	12.44	12.58	12.44
eEye DS Blink	16.83	1.23	1.23	1.23	3.55	3.56	3.55	4.98	10.39	10.20	3.13	3.11	3.13
Emsisoft Anti-Malware	3.25	3.00	26.19	3.00	0.68	1.45	0.68	0.33	1.57	0.68	0.35	11.51	0.35
eScan IS Suite	3.25	3.00	26.19	3.00	0.68	1.45	0.68	0.33	1.57	0.68	0.35	11.51	0.35
ESET NOD32 Antivirus	61.36	4.10	4.12	4.10	48.77	51.85	48.77	14.75	32.84	30.22	10.30	11.27	10.30
Fortinet FortiClient	15.05	8.17	8.45	8.17	9.28	9.42	9.28	6.55	13.72	13.42	11.51	11.63	11.51
Frisk F-PROT	29.67	9.38	9.32	9.38	15.54	15.54	15.54	12.02	26.48	24.63	17.74	18.66	17.74
F-Secure Client Security	22.96	9.17	2906.94	7.57	25.26	2463.05	25.79	31.23	2463.05	30.60	72.13	1082.01	17.17
G Data AntiVirus	33.93	5.07	2906.94	5.07	23.46	2463.05	23.46	13.90	1642.04	28.47	270.50	360.67	6.25
GFI VIPRE Antivirus	8.83	3.21	3.19	3.21	22.70	23.68	22.70	4.03	8.31	8.25	1.86	1.86	1.86

* System drive size measured before product installation

(Please refer to text for full product names)

the large scan of the full selection of sets trundling along for over eight full days. Thankfully, there was no instability and logging was maintained well throughout.

Detection rates were good in the main sets, dwindling somewhat through the RAP sets, but the WildList was well handled and there were no issues in the clean sets, earning *Defenx* another VB100 award. The vendor has five passes in the last six tests, having skipped the annual *Linux* comparative, and eight passes since its first entry nine tests ago. No stability problems were noted this month, but the slow scanning speed meant more than ten days' test machine time was used to complete all our work.

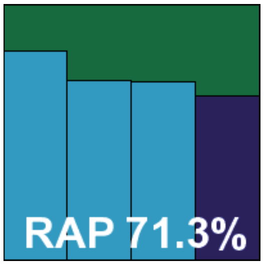
Digital Defender Antivirus Pro

Version 2.1.68, Definitions version 14.0.90

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.61%
Worms & bots	91.69%	**False positives**	0

The second of this month's set of products based on the *Preventon* SDK and *VirusBuster* engine, *Digital Defender* has become a fairly regular sight on our test bench. The 63MB installer runs through in good time, requiring web access to run and apply a licence key, and needing no reboot to complete. The GUI is sparse and simple, with basic controls only, but is perfectly usable for the undemanding user. As with the rest of this range, logging is somewhat troublesome, defaulting to 'Extended Logging' which means that every item looked at is noted down in the logs. To combat the bloating effects of this, logs are abandoned after reaching a few MB in size, or a few thousand files scanned, and while the verbosity can be switched off from the GUI, a registry tweak is required to prevent logs from being dumped.

vb 100 VIRUS virusbtn.com Aug 2011



With this done, and a reboot performed for the setting change to take effect, tests moved along nicely with no problems. One minor issue we observed was that changes to the settings for on-demand scans seem only to affect scans run from within the product GUI, while right-click scans continue to use the default set of options.

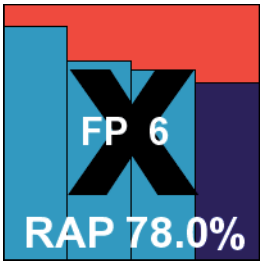
Speeds were not bad, and overheads not heavy, with low use of resources and little effect on the running time of our set of tasks. Detection rates were decent if not stellar, and with the WildList and clean sets handled properly, another VB100 award goes to *Digital Defender*. The vendor's history shows a period of recovery after a rocky spell, with three passes, two fails and one no-entry in the last six tests, four passes and four fails since its first entry nine tests ago. With no crashes or stability problems, all tests completed in a little over 24 hours, just about on schedule.

eEye Digital Security Blink Professional

Version 4.8.2, Rule version 1622, Antivirus version 1.1.1560

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	94.19%
Worms & bots	93.18%	**False positives**	6

Another product using an OEM engine, *eEye*'s *Blink* includes *Norman*'s detection technology alongside the company's own vulnerability expertise. The product installer is a sizeable 176MB, accompanied by an additional 116MB of offline updates, but it trips through rapidly, with half a dozen clicks and no need to reboot.



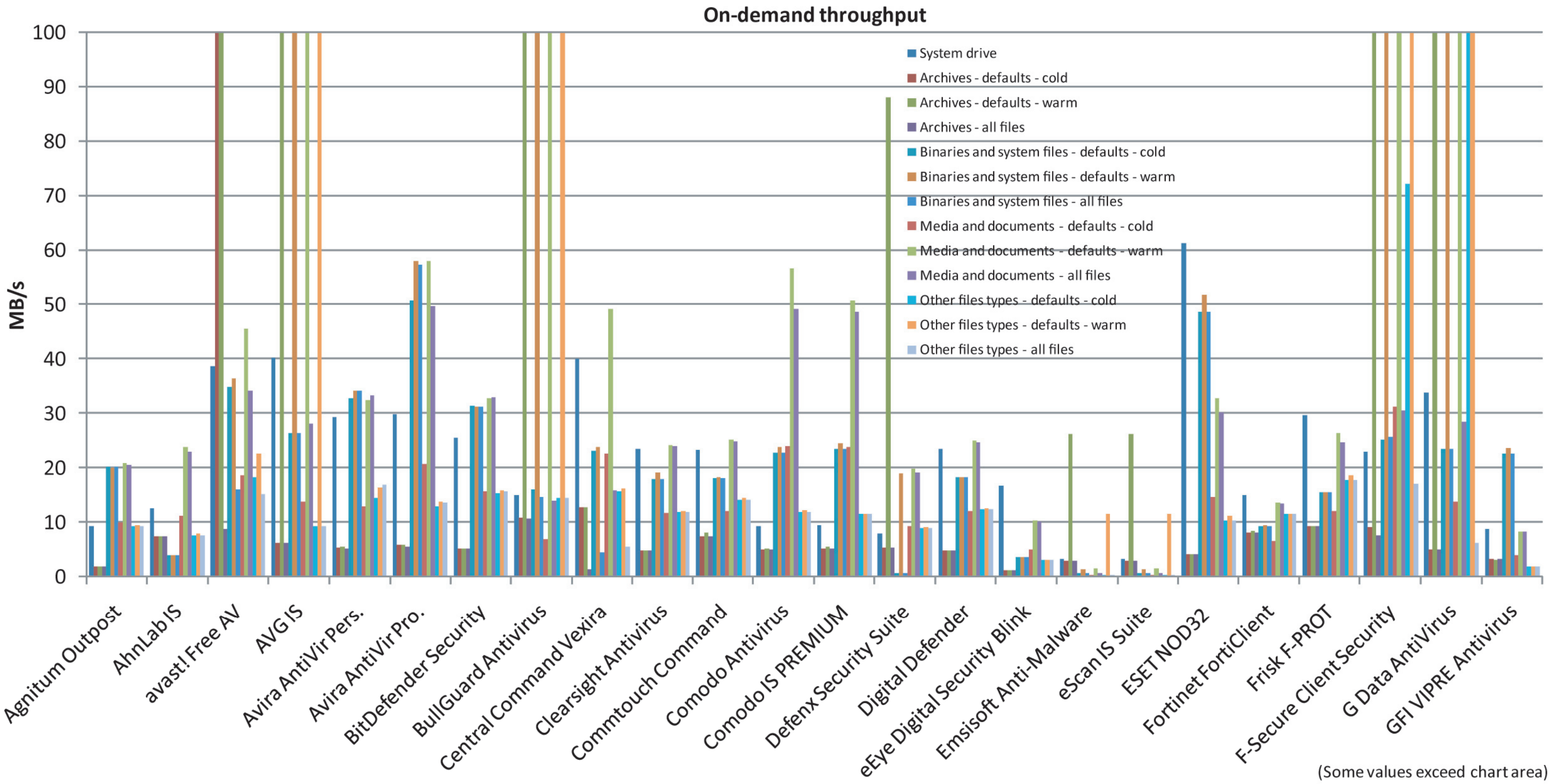
The interface features warm colours and a friendly layout, with a mysterious black-hatted figure icon representing the anti-malware component, which runs alongside the vulnerability management, firewall, intrusion prevention and other features. Controls are not as complete as in some solutions, but provide a reasonable degree of fine-tuning, and tests ran through reasonably quickly and without too much trouble.

Scanning speeds were slow, perhaps in part due to the sandboxing system, with fairly hefty overheads on access too. However, use of RAM wasn't too heavy, while CPU use was a little above average and impact on our set of tasks was noticeable but not overly intrusive. Detection rates were decent in the main sets, a little less impressive in the later weeks of the RAP sets, but the WildList caused no problems. The clean sets threw up a number of alerts, several of which were for suspicious items, but a few described clean items as malware. These included a component of the *ICQ* chat program and, slightly more controversially, a handful of files from a leading PC optimization suite – which a few other programs this month labelled as potentially unwanted and some have described as having 'dubious value' – were labelled W32/Agent, which was adjudged a step too far.

On-demand throughput contd. (MB/s)	System drive*	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
Ikarus virus.utilities	23.12	20.19	20.91	20.19	19.86	19.78	19.86	18.93	38.19	38.79	16.39	16.91	16.39
Iolo System Shield	27.73	8.97	9.00	8.97	17.47	17.35	17.47	12.39	25.66	25.39	21.22	21.22	21.22
Kaspersky IS 2012	90.26	6.97	2906.94	6.97	41.75	2463.05	41.75	22.68	821.02	46.47	19.67	360.67	19.67
Kaspersky SO Security 2	51.49	7.34	1453.47	7.34	41.05	615.76	41.05	18.93	234.58	38.79	18.66	120.22	18.66
Lavasoft Ad-Aware TS	27.28	4.60	2906.94	4.60	18.11	821.02	18.11	13.07	223.91	26.77	10.93	154.57	10.93
LogicOcean Gprotect	26.09	4.74	4.77	4.74	19.09	19.24	19.09	11.90	25.01	24.39	13.04	13.20	13.04
McAfee VirusScan	13.39	15.55	29.36	15.55	41.05	117.29	41.05	20.73	120.15	42.47	23.02	98.36	23.02
Microsoft SE	40.52	4.65	4.84	4.65	14.62	16.70	14.62	17.81	46.92	36.49	15.68	18.03	15.68
Norman Security Suite	15.81	1.23	1.26	1.23	5.08	5.34	5.08	6.57	14.62	13.46	5.61	5.64	5.61
PC Booster AV Booster	24.87	4.68	4.70	4.68	21.23	21.51	21.23	12.27	24.15	25.13	12.73	12.88	12.73
PC Tools Internet Security	46.11	8.52	2906.94	5.54	164.20	821.02	164.20	10.78	289.77	22.09	10.50	120.22	10.50
PC Tools SD with AV	44.11	8.45	581.39	8.45	246.31	447.83	246.31	11.08	214.18	22.70	9.66	72.13	9.66
Preventon	23.22	9.50	9.56	9.50	18.66	18.80	18.66	11.79	24.27	24.15	12.02	12.16	12.02
Qihoo 360 Antivirus	29.93	4.29	4.36	4.29	19.47	19.63	19.47	10.10	23.35	20.70	10.02	10.50	10.02
Quick Heal Antivirus Pro	26.57	2.36	2.35	2.32	35.70	37.32	36.76	9.25	19.17	19.24	9.49	10.30	10.30
Returnil System Safe	22.87	4.55	5.44	4.55	10.69	11.09	10.69	4.86	10.31	9.95	7.62	8.39	7.62
Rising Internet Security	24.33	1.31	1.33	1.31	11.96	12.19	11.96	9.90	20.36	20.27	11.63	11.63	11.63
Security Coverage SecureIT	23.78	181.68	181.68	5.97	28.47	29.32	19.02	14.48	31.99	29.32	13.53	12.88	12.88
Sophos ESC	17.34	1.62	1.62	1.62	20.19	19.78	20.19	15.03	30.98	30.79	10.11	10.02	10.11
SPAMfighter VIRUSfighter	23.24	3.79	4.11	NA	17.66	17.85	17.66	10.15	22.91	20.79	11.39	11.39	11.39
Total Defense ISS Plus	44.70	4.73	2906.94	4.73	29.32	2463.05	29.32	23.12	821.02	47.37	21.22	270.50	21.22
Total Defense TD r12	67.37	207.64	2906.94	3.96	41.05	2463.05	38.79	23.81	985.22	46.04	19.32	270.50	18.66
TrustPort Antivirus 2012	10.99	2.55	2.48	2.55	15.44	15.49	15.44	7.94	16.64	16.26	5.61	5.72	5.61
VirusBuster Professional	40.24	12.53	12.69	1.40	22.81	24.03	4.44	22.47	51.31	15.79	15.46	17.17	5.46

* System drive size measured before product installation

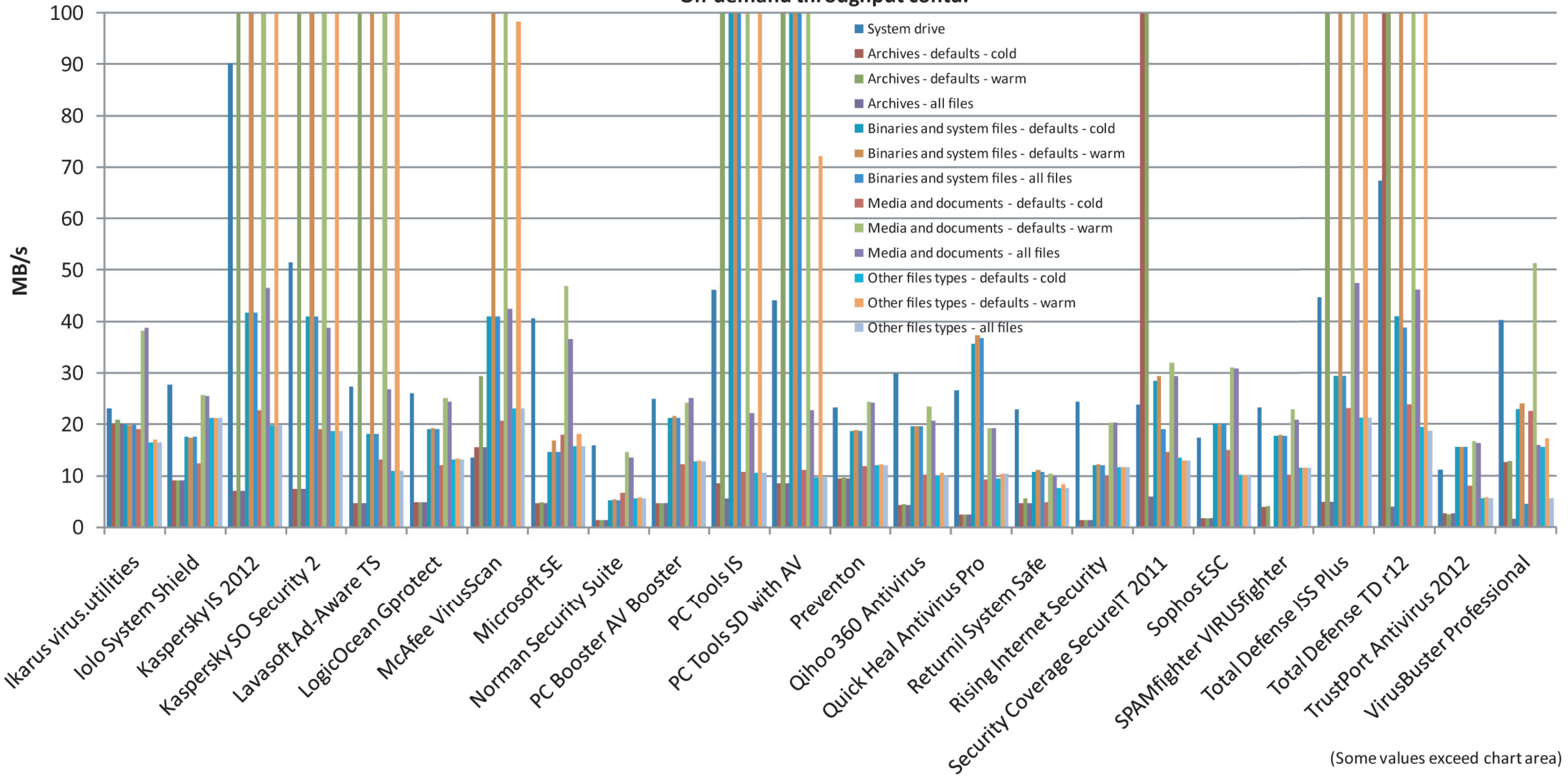
(Please refer to text for full product names)



(Some values exceed chart area)

(Please refer to text for full product names)

On-demand throughput contd.



(Some values exceed chart area)

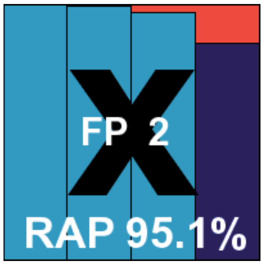
(Please refer to text for full product names)

As a result, there is no VB100 award for *eEye* this month, the vendor's history now showing three passes, two fails and one no-entry in the last six tests; three passes, five fails and four tests skipped in the last two years. With no stability problems, slow scanning times were the only issue this month, causing the full set of tests to take around two days to complete.

Emsisoft Anti-Malware

Version 5.1.0.15, Malware signatures 5,511,662

ItW	100.00%	**Polymorphic**	95.80%
ItW (o/a)	100.00%	**Trojans**	99.61%
Worms & bots	99.44%	**False positives**	2



Emsisoft's solution, formerly known as 'A-Squared', includes the *Ikarus* detection engine alongside some of its own stuff. The installer isn't too large though, at 109MB with all updates included, and the set-up process is fairly speedy, with a few more clicks required than some, but no reboot. The initial install is followed by a set-up wizard with some further options, and things are quickly up and running.

The GUI is a little unusual in the way it switches between areas, leading to occasional confusion, and some of the options are perhaps not as clear as they could be, but it is generally usable, providing a basic set of options. Running seemed stable in the on-demand tests, showing some fairly slow scanning speeds, but the on-access component was decidedly flaky – running fine for a while but regularly bringing whatever test was running to a halt; while the cursor could be moved around the screen after one of these freezes, the system refused to respond otherwise, and only a hard reboot got things moving again. This occurred most often during the runs over the infected sets, but was also observed a few times when running the standard speed and performance measures, using only clean samples and fairly standard actions.

When we finally got all the tests completed, after several runs through and several re-installs, we saw some surprisingly light overheads for the on-access measures, with low use of RAM and unexceptional use of CPU cycles and impact on our set of tasks. Detection rates, meanwhile, were excellent, with superb coverage in all sets, even the proactive part of the RAP sets handled admirably. The WildList was brushed aside effortlessly, but in the clean sets a couple of items – one of them a driving simulation game – were alerted on as malware, denying *Emsisoft* a VB100 award this month.

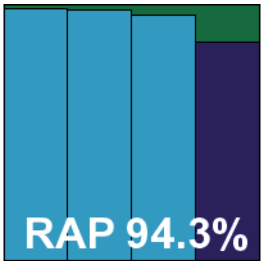
The vendor's test record is a little rocky of late, with one pass and four fails in the last six tests, the annual *Linux* test having been skipped. Since its first entry nine tests ago, it has managed two passes, with five fails and two tests having been skipped. There were some clear problems with the on-access component in this test, freezing the system when under pressure on several occasions, and the retesting this necessitated meant that more than three full days were taken up.

eScan Internet Security Suite

Version 11.0.1139.1003

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.48%
Worms & bots	99.62%	**False positives**	0

vb 100 VIRUS virusbtn.com Aug 2011



A long-term regular, *eScan* is rarely absent from our tests. This month's product came as a large 172MB installer, although all updates were included. The set-up process was a little lengthy, needing no reboot to complete but still taking a fair while. When the system was rebooted for other purposes, the UAC subsystem popped up several warnings about the mail scanning components.

The interface is bright and flashy, with a slick animated bar of icons along the bottom, but the layout is clear and logical, making navigation easy. Excellent configuration is available under the shiny covers in a much more sober and logical style.

Scanning speeds were slow, with several scans taking more than the maximum allotted two hours, including scans of the local C: partition. Meanwhile, the scan of the clean sets – which many products got through in the space of a morning – took over 58 hours to complete. On access things were a little better, with pleasantly light overheads, and use of resources and impact on our set of activities were notably on the low side.

Detection rates were splendid though, thanks to the underlying *BitDefender* engine, with all sets covered excellently. The WildList caused no problems, and the clean sets were handled well, earning *eScan* another VB100 award;

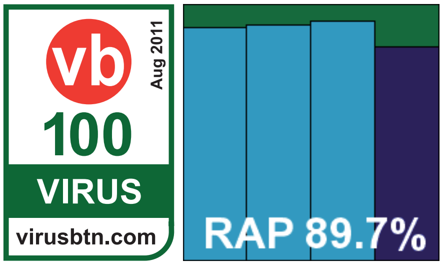
the vendor now boasts five passes and a single fail in the last six tests; nine passes and three fails in the last two years.

Stability seemed fine for the most part, but some of the scans were extremely slow, meaning the total testing time was more than five days.

ESET NOD32 Antivirus 4

Version 4.2.71.2, Virus signature database 6229

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.36%
Worms & bots	96.70%	**False positives**	0



Still maintaining the record for the longest run of passes, *ESET* is one of our most regular participants. The latest product version was provided as a fairly small 51MB package, including all required updates, and installed in a handful of standard steps, enlivened only by the usual step of forcing a decision on whether or not to detect ‘potentially unwanted’ items. The process doesn’t take long, and needs no reboot to finish.

The interface is attractive and elegant, glossy without losing a sense of solid quality. Configuration is provided in massive depth and is generally easy to navigate if seeming a little repetitive in places. Operation was pretty straightforward, with no problems with stability. Scanning speeds were pretty fast and very consistent, while on-access overheads were light, resource consumption average and impact on our activities not too heavy.

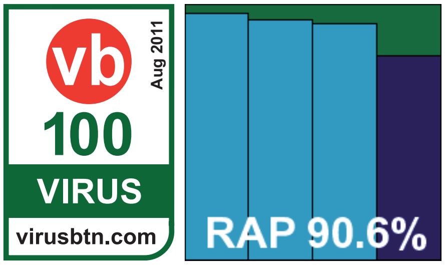
Detection rates were decent, with again impressive consistency across the weeks of the RAP sets. The clean sets did throw up a fair number of alerts – mostly for toolbars and adware bundled with freeware packages, but also several items from a suite of system cleaning and optimization tools were labelled as potentially unwanted (the same items having been described by another vendor as having ‘dubious usefulness’).

None of these could be described as a false alarm though, as the descriptions were pretty accurate, and with the WildList handled well *ESET* comfortably maintains its unbroken record of VB100 passes, having entered and passed every test since the summer of 2003. With no crashes or other problems of any sort, and good speeds, all tests were comfortably completed within 24 hours.

Fortinet FortiClient

FortiClient version 4.1.3.143, Virus signatures version 10.855, AntiVirus engine 4.3.366

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.87%
Worms & bots	97.39%	**False positives**	0



Fortinet’s showings in our tests have been steadily improving of late, and we looked forward to seeing if it could maintain this impressive trend. The submission took the form of a tiny 10MB main installer, with 126MB of updates in a separate bundle, and the install process was very fast and simple, running through the standard steps in good time with no reboot required. The interface is efficient and businesslike, with a good level of fine-tuning but little chance of getting lost amongst the clear, simple dialogs. Operation seemed smooth and reliable, and tests proceeded without incident.

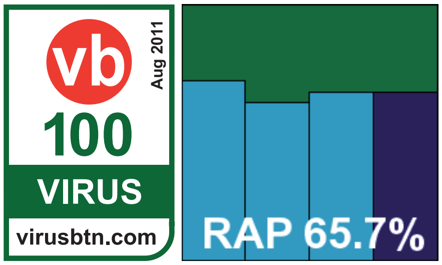
Scanning speeds were fairly average, but overheads were light, although CPU use was a little high; RAM use and impact on our set of tasks were around average for this test. Detection rates showed that the upward trend has not yet reached an end, with some very impressive figures across all the sets. While the RAP sets trailed off a little into the later weeks, scores remained pretty decent. The WildList and clean sets presented no problems, and *Fortinet* earns a VB100 award.

The vendor now has four passes and a single fail in the last six tests, the annual *Linux* test having been skipped; seven passes and three fails over the last two years, again just missing the *Linux* comparatives. With no stability problems this month and good speeds, all tests were completed within 24 hours.

Frisk F-PROT Antivirus for Windows

Version number 6.0.9.5, Scanning engine version number 4.6.2, Virus signature file from 19/06/2011, 20:48

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	79.13%
Worms & bots	74.27%	**False positives**	0



Another long-term regular, *F-PROT* has been a reliable and seldom changing entrant for many years now. The current product is a compact 31MB installer with 27MB of updates, and installs in just a few steps, finishing very quickly but needing a reboot to finish off. The interface is simple in the extreme with only the bare minimum of controls, but is pretty easy to use and tests proceeded well.

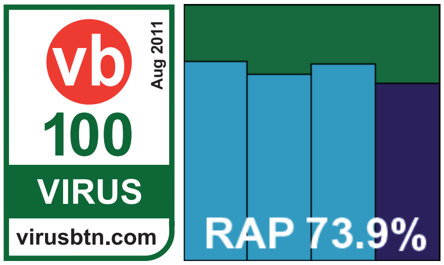
Scanning speeds were not bad, although overheads seemed a little high on access. Use of memory and processor cycles was low, with only a small effect on the runtime of our set of tasks. Detection rates were not the highest, but were reasonably decent in most sets, with the core certification sets handled well and a VB100 award is comfortably earned.

Frisk now has four passes and two fails in the last six tests; seven passes and five fails in the last two years, with all comparatives entered. With little fuss and no crashes or other problems, all tests completed comfortably within the one-day target time.

F-Secure Client Security

Version 911 build 411

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.78%
Worms & bots	99.51%	**False positives**	0



F-Secure's *Client Security* line appears designed for business use, with the installer (63MB, with 139MB of updates) providing options to connect to a central management system for policy control, although of course we opted for a standalone version. Other installation stages were more standard, and the process completed in reasonable time, with a reboot at the end.

The product interface is pretty pared down, with little configuration made available to the end-user, although presumably a centrally managed version will have more options for the administrator to impose fine control. It is fairly easy to use, although we did note a few problems: the custom scan failed to do anything several times and there was some rather odd behaviour when we did manage to start scans. Several times, we noted scans claiming to have completed, but recording much lower numbers of files scanned than we would expect – implying that the scanner was giving up part-way through the job assigned to it. In some cases, it seemed that the number reported could not represent the actual number scanned either, suggesting that the reporting system first counts the number of files in a folder, adding that to its total so far, then claims that total as completed even if the scan gives up halfway through the folder in question.

Scanning speeds proved to be reasonable on first attempt with huge improvements in the warm runs, with on-access speeds similarly impressive, while all our resource use measures were very low and our set of tasks zipped through very quickly.

After several repeat runs, we got together what seemed to be a full set of results from the infected sets too, but with the reports clearly misleading it was hard to tell if everything had in fact been covered. On processing the figures, RAP scores were lower than we would expect from the product, with several other solutions using the same *BitDefender* engine doing much better this month, but with limited time we could not retest further to get closer to the truth.

The core certification sets were well handled though (the clean sets were run through on access to ensure no lurking false alarms had been skipped over by the flighty scanner), and a VB100 award is just about earned; this brings *F-Secure*'s recent record to four passes in the last six tests, with two tests skipped; nine passes and three no-entries in the last two years. The suspect scanning and logging behaviour, and resulting multiple retests, meant the product took up nearly five full days of testing time.

G Data AntiVirus 2012

Version 22.0.2.38

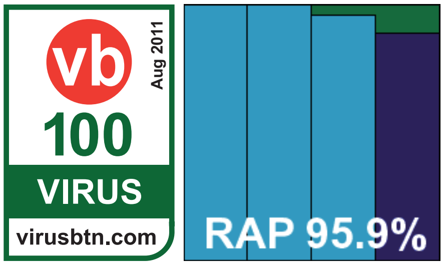
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.83%
Worms & bots	99.92%	**False positives**	0

G Data's 2012 edition isn't greatly different from the previous version, with the very hefty 346MB install package taking slightly more than the usual number of clicks to run through, with a reboot needed at the end. The interface is simple and clear, but has a wealth of fine-tuning tucked away beneath the surface, all presented in a pleasant and easy-to-use style.

File access lag time (s/GB)	System drive*	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	22.94	7.35	7.04	NA	36.43	35.51	36.43	67.83	65.86	67.83	92.04	90.30	92.04
AhnLab IS	81.42	22.58	23.07	NA	320.49	318.41	320.49	60.62	60.57	60.62	97.25	96.89	97.25
Avast Software avast!	6.51	1.44	0.23	74.93	10.81	0.76	8.05	12.89	0.45	9.48	57.86	18.59	44.92
AVG Internet Security	4.23	11.72	9.09	NA	38.18	6.31	7.08	88.81	21.86	34.63	94.09	13.20	37.21
Avira AntiVir Pers.	19.72	14.68	11.08	85.79	22.18	6.24	25.16	50.85	37.92	50.04	47.26	45.96	46.09
Avira AntiVir Pro.	10.50	14.63	11.53	46.61	16.38	5.71	22.40	50.75	36.13	50.09	46.55	45.92	46.34
BitDefender Security	6.22	146.20	1.71	143.82	25.65	1.03	25.42	41.14	0.75	40.67	49.21	1.79	47.43
BullGuard Antivirus	9.16	97.17	29.24	NA	35.51	5.70	35.51	69.51	16.07	69.51	71.70	10.36	71.70
Central Command Vexira	18.28	1.46	1.27	NA	33.67	33.85	33.67	30.61	30.54	30.61	108.72	77.27	108.72
Clearsight Antivirus	23.04	28.58	28.75	NA	42.29	44.98	49.32	10.65	10.01	79.87	17.83	17.43	71.99
Commtouch Command	20.00	84.01	84.79	7.64	52.50	49.09	57.25	103.08	96.95	2.17	95.16	93.18	66.52
Comodo Antivirus	18.26	2.62	2.54	NA	56.81	51.52	56.81	11.99	7.23	11.99	134.26	124.27	134.26
Comodo IS PREMIUM	14.52	1.75	1.69	NA	52.08	50.88	52.08	15.75	13.80	15.75	128.65	125.35	128.65
Defenx Security Suite	75.09	11.25	180.25	NA	77.63	793.85	77.63	946.72	4807.62	946.72	2380.71	7456.67	2380.71
Digital Defender	22.56	30.85	31.37	NA	46.57	46.40	43.39	7.90	7.85	66.66	13.97	13.14	65.09
eEye DS Blink	31.23	3.41	4.49	609.41	64.25	63.35	61.28	173.79	172.45	174.27	264.87	263.90	265.51
Emsisoft Anti-Malware	1.89	0.62	0.10	60.42	4.69	2.76	20.21	9.32	7.35	41.90	10.93	10.47	60.08
eScan IS Suite	11.32	7.50	1.89	60.42	25.41	3.93	20.21	54.82	4.61	41.90	88.60	6.81	60.08
ESET NOD32 Antivirus	4.71	1.14	0.12	2.61	0.56	0.15	12.20	41.40	38.93	41.35	62.66	60.63	71.70
Fortinet FortiClient	34.52	91.61	2.33	2.33	52.69	0.15	52.69	31.12	0.92	31.12	46.94	2.01	46.94
Frisk F-PROT	15.89	14.12	14.48	NA	58.12	56.44	58.12	34.62	31.89	34.62	48.60	37.96	48.60
F-Secure Client Security	8.25	11.18	10.27	NA	52.68	5.75	NA	73.31	16.82	NA	27.02	8.98	NA
G Data AntiVirus	21.29	33.82	5.38	5.38	45.10	10.58	45.10	97.92	33.44	97.92	207.31	18.52	207.31
GFI VIPRE Antivirus	2.48	4.92	4.37	NA	31.11	3.11	31.11	453.16	14.50	453.16	423.42	19.34	423.42

* System drive size measured before product installation

(Please refer to text for full product names)



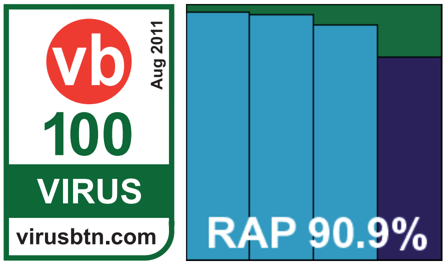
Initial scan times were a little slower than many, as might be expected from a multi-engine product, but some very efficient optimization meant repeat scans blazed through very quickly, and on-access measures also improved greatly, from a reasonable starting point. Resource use was low, particularly CPU use, but for some reason our suite of tasks took quite some extra time to run through.

Detection rates were as eye-opening as ever, with splendid coverage across the sets, pushing very close to 100% in all but the latest weeks of the RAP sets. The WildList was demolished and the clean sets left untouched, easily earning *G Data* another VB100 award. The vendor's record stands at four passes and a single fail in the last year, with no entry in the *Linux* test; eight passes and two fails in the last two years, with two tests (both on *Linux*) not entered. Stability was solid as a rock throughout testing, and thanks to the splendid use of optimization techniques all our tests completed well on schedule, in less than 24 hours.

GFI VIPRE Antivirus

Software version 4.4.4194, Definitions version 9660, VIPRE engine version 3.9.2495.2

ItW	100.00%	**Polymorphic**	99.80%
ItW (o/a)	100.00%	**Trojans**	96.95%
Worms & bots	97.24%	**False positives**	0



With the takeover of Florida's *Sunbelt Software* by Malta-based *GFI* a few months back, we've finally managed to adjust our systems to correctly reference the new company name, and put it in the right order alphabetically. The product is largely unchanged though, and still bares *Sunbelt* rather than *GFI* branding in most places. The product installer is compact at just 13MB, with updates of 68MB. The set-up process is pretty straightforward but does have a few longish pauses. A reboot is required, which is followed by some initial configuration steps. Our first attempt brought some warnings that the on-access component could not be started after the reboot, but a second reboot soon fixed things; the same issue re-emerged on a subsequent install too.

The interface is simple, unflashy and a little text-heavy, but is fairly easy to find one's way around, providing a little more than the minimum set of controls, but not as much as some. Some of the options are a little less than clear at first glance, but usage is not too difficult after a little experimentation. Scanning speeds were pretty slow, and access overheads a little heavy in some areas, but resource use was tiny and our set of tasks ran through almost unimpeded.

Scanning our infected sets is always a little tricky with *VIPRE*, it being another product that takes the rather suspect route of storing all detection data in memory until the end of a scan. Thus, when scans fail (as they did regularly this month, with an error message reading starkly 'Your scan has failed'), not a scrap of data can be retrieved. Attempts to get through all but the smallest sub-division of our sets led to problems, with large amounts of memory being eaten up, so we had to run many little tests and pile all the results together at the end.

Detection rates, once pulled out of rather unwieldy logs, showed some decent scores with good levels across the main and RAP sets, dropping a little in the proactive RAP week as expected. The core certification sets were well handled, and *GFI* (formerly *Sunbelt*) earns a VB100 award.

VIPRE now has four passes in the last six tests, having skipped two, and six passes and one fail in the last two years, with the rest not entered. Other than the odd reboot issue after installation, and the problems scanning large infected sets, there were no other stability problems, but with the extra work imposed by large scans failing, and the many repeat runs required, testing took around six days to complete.

Ikarus virus.utilities

Product version 2.0.42, Virus database version 78656

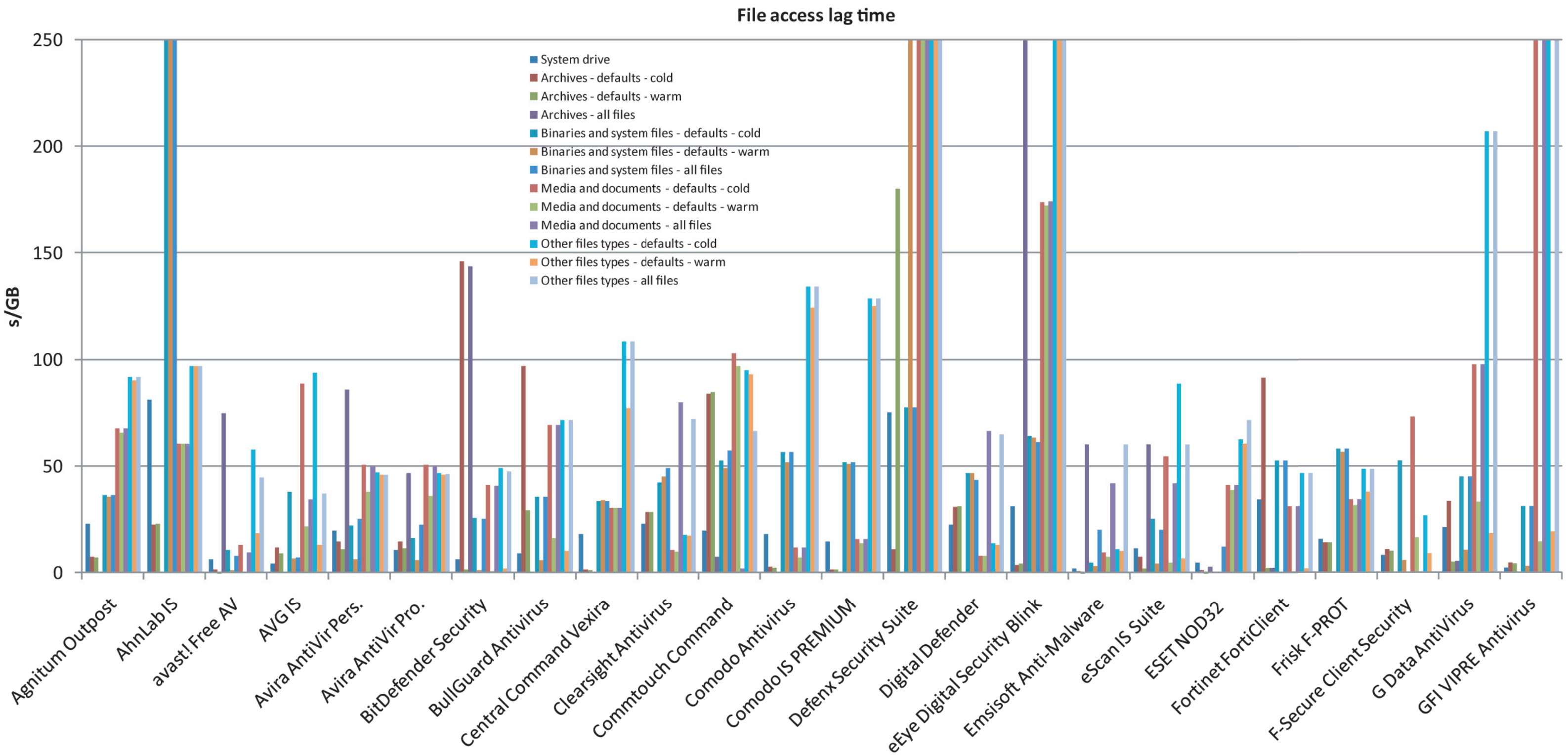
ItW	100.00%	**Polymorphic**	95.80%
ItW (o/a)	100.00%	**Trojans**	99.56%
Worms & bots	99.31%	**False positives**	2

Another pretty compact product, the install package sent in by *Ikarus* measured just 18MB, although an additional 68MB of updates was also provided. The install system was clear and well explained, but needed around a dozen clicks to complete, making it one of the longer set-up processes this month. No reboot was needed though, and the actual business of putting files and settings in place was pretty speedy.

File access lag time contd. (s/GB)	System drive*	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
Ikarus virus.utilities	16.54	41.76	44.82	NA	40.00	39.43	40.00	28.13	27.64	28.13	43.53	42.39	43.53
Iolo System Shield	22.48	89.31	94.27	89.31	57.26	51.81	57.26	114.69	108.02	114.69	74.84	65.63	74.84
Kaspersky IS 2012	13.91	6.25	2.06	NA	38.32	4.99	38.31	55.98	8.80	59.94	80.10	12.37	83.68
Kaspersky SO Security 2	11.22	0.99	0.56	1.74	2.28	1.10	1.46	14.84	8.55	16.90	10.97	5.50	16.33
Lavasoft Ad-Aware TS	18.04	43.59	1.91	314.63	76.98	6.09	84.67	90.50	9.56	96.51	125.17	15.58	133.62
LogicOcean Gprotect	17.87	30.42	30.73	195.03	44.00	43.96	43.74	13.53	12.94	67.80	12.33	11.53	65.86
McAfee VirusScan	13.72	4.56	3.53	415.75	61.14	27.70	65.75	90.06	42.14	83.63	127.29	67.42	128.55
Microsoft SE	0.68	14.36	10.42	NA	61.04	6.29	61.04	45.86	18.61	45.86	49.96	10.20	49.96
Norman Security Suite	41.16	6.37	7.84	NA	72.56	74.29	72.56	203.46	200.45	203.46	256.00	252.79	256.00
PC Booster AV Booster	23.92	27.94	28.03	181.93	37.52	37.42	37.28	3.50	3.97	58.45	9.74	10.34	66.16
PC Tools Internet Security	3.94	4.39	14.98	NA	44.53	11.14	NA	49.44	35.62	NA	26.87	6.99	NA
PC Tools SD with AV	3.63	17.68	10.51	NA	46.44	8.00	NA	70.00	42.31	NA	43.28	25.12	NA
Preventon	19.98	29.08	29.06	183.86	45.05	44.90	44.27	9.53	9.50	63.36	16.79	16.52	69.64
Qihoo 360 Antivirus	4.22	4.03	2.84	NA	8.91	10.74	NA	54.65	64.36	NA	52.32	64.82	NA
Quick Heal Antivirus Pro	10.49	36.39	0.07	41.36	13.65	2.52	19.65	72.67	8.59	81.18	75.23	12.32	80.48
Returnil System Safe	20.03	23.26	29.68	NA	54.67	58.29	54.67	122.91	124.99	122.91	60.38	56.99	60.38
Rising Internet Security	18.53	38.92	26.50	NA	63.19	4.97	63.19	87.61	70.29	87.61	80.45	52.26	80.45
Security Coverage SecureIT	8.36	112.48	0.10	112.48	30.49	2.86	30.49	45.18	8.73	45.18	59.62	12.57	59.62
Sophos ESC	22.01	1.17	1.16	577.14	36.97	36.59	45.76	23.85	23.80	30.23	58.29	58.20	70.30
SPAMfighter VIRUSfighter	21.03	27.71	27.65	135.64	45.38	45.16	44.92	10.86	10.65	62.97	18.47	18.36	72.48
Total Defense ISS Plus	16.86	2.69	2.11	NA	28.12	23.47	28.12	28.25	25.65	28.25	31.00	28.23	31.00
Total Defense TD r12	19.27	4.21	3.59	NA	19.34	16.49	19.34	128.85	125.25	128.85	172.25	170.62	172.25
TrustPort Antivirus 2012	17.06	6.25	2.06	275.60	38.32	4.99	38.31	55.98	8.80	59.94	80.10	12.37	83.68
VirusBuster Professional	15.93	1.55	0.51	4.60	41.64	23.65	53.02	19.53	18.95	53.05	60.51	57.70	85.68

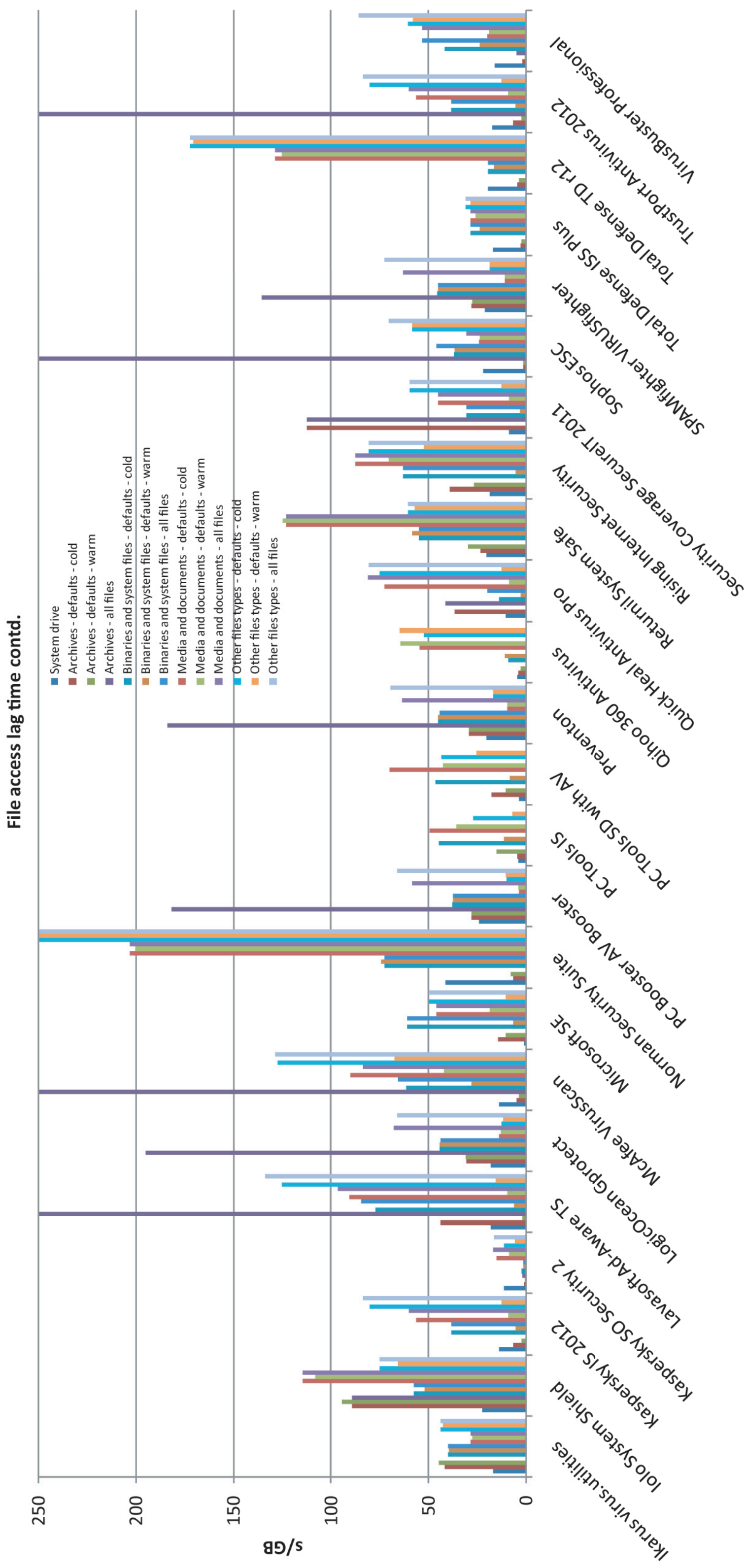
* System drive size measured before product installation

(Please refer to text for full product names)



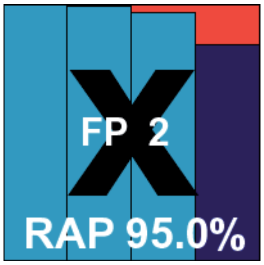
(Some values exced chart area)

(Please refer to text for full product names)



(Some values exced chart area)

(Please refer to text for full product names)



The interface is simple and minimalist – one of few to make use of the .NET framework for its displays – and has been somewhat flaky in the past, but this month it ran fairly stably on the whole. Operation is reasonably straightforward, and testing proceeded well, but part way through one test the power in the lab died unexpectedly, causing some rather nasty problems. The test system failed to boot even as far as the logon screen, on several attempts, but booting into safe mode and disabling the guard process fixed things relatively easily.

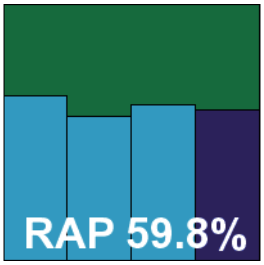
Scanning speeds were pretty good, and on-access overheads not bad either, with low RAM use, medium use of CPU cycles, and an average impact on our set of tasks. Detection rates were extremely high, challenging the very best in this month's test, but this excellent coverage of malware was counterbalanced by a couple of false alarms in the clean sets, as happened to another product using the same engine earlier. The developers informed us that at least one of the issues had already been fixed some time before we told them about it, but no VB100 award can be granted this month.

The product's history now shows one pass and three fails in the last six tests, with two not entered; two passes and five fails over the past two years, with five tests skipped. There were no stability issues other than the bootup problems following the power outage, and testing ran through in very good time, comfortably under our 24-hour goal.

Iolo System Shield

Version 4.2.4

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	73.44%
Worms & bots	70.28%	**False positives**	0



With anti-malware protection based on the *Frisk* engine – already successful this month in a number of other forms – *Iolo*'s chances for success looked good from the off. The product arrived initially as a tiny downloader of less than 500KB, which proceeded to fetch the full 48MB install package from the Internet, taking seven to eight minutes. An offer is made to keep a copy of this file in case of future reinstalls, which we thought was rather a sensible move. The set-up follows the usual lines, taking only about a minute to complete, and requests a reboot at the end. An update is then run, completing very quickly, and all is good to go.

The product interface is crisp and professional-looking, with no surprises and a sensible, logical layout. A reasonable if not exhaustive level of configuration is provided, which is clear and easy to use. Options to respond to detections by logging or blocking access only, which are preferred for our testing, were sadly absent, so we resorted to allowing the product to rename. This involved changing the file extensions of detected items to '.INFECTED'. Logs could not be exported from the product interface, and despite an urgent request for information from the developers (not the first time such a request has been submitted), the bizarre log format refused to yield its secrets. Some manual hacking of the file produced some usable data, which was compared with the lists of renamed files in our sets to confirm accuracy.

Scanning speeds were not bad, but on-access overheads were noticeably heavier than most, with heavy use of CPU cycles and a significant impact on our test of activities. RAM use, rather oddly, was high with the system idle, but more normal when hectic file processing was going on.

Detection rates, when finally deciphered, were unspectacular at best, and poorer than expected in the RAP sets, which implies that we may not have made as good a job as we thought of spotting all detections. Nevertheless, the WildList was well managed, and the clean sets confirmed to be properly handled, earning *Iolo* a VB100 award.

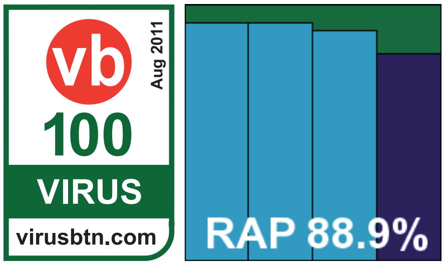
The product has made only sporadic appearances in our tests, with one pass and two fails from three entries in the last six; one pass and three fails from four attempts in the past two years. There were no crashes or stability problems, and testing did not take too long, even factoring in the time needed to set our test sets back to normal and to process the log data. Everything was dealt with in about 36 hours.

Kaspersky Internet Security 2012

Version 12.0.0.374 (a)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.54%
Worms & bots	93.84%	**False positives**	0

There was much excitement in the lab at seeing the latest offering from *Kaspersky Lab*, the 2012 product hitting the market good and early. Initial impressions were good, with



the mid-sized 68MB installer running through with a minimum of interaction and maximum of speed, getting everything ready in excellent time. Updates were applied from a large bundle containing data for the company's full product line.

The interface is very slick and attractive – a little quirky as usual, but quickly becoming easy to operate. Configuration for the huge range of components is exemplary in its detail and clarity, making it very simple to take complete control of how protection is implemented.

Running through the tests was pretty impressive at first, with good initial scan times becoming lightning fast in the warm runs, and similarly superb speeds in the on-access tests. Resource use was low, and our suite of activities took very little extra time to complete.

On-access detection tests powered through and showed the expected solid scores, and on-demand scans completed overnight with no problems. Trying to view the results, however, proved something of a problem. With the report database measuring around 400MB, it seemed too much for the product to handle, and we decided to reboot to clear the air a little. With the system up and running, we found the product failing to open, and tried again. After some investigation, and discussion with the developers, it emerged that such large logs were expected to cause significant delays in starting the product (which seems to need to load in all log data before it can get going). Leaving it overnight, we saw it using up almost 1GB of memory, but the interface still crashed whenever we tried to open it. Of course, our test scenarios are far outside the normal usage pattern of the product, but we would expect QA procedures to include some heavy stress testing to ensure this sort of edge case cannot completely disable the product.

Trying to move on, we looked at the log database, only to find yet another gnarly and awkward proprietary format had been used. Contacting the developers once again, we were informed that no information was available on the format of the database, and that no tool other than the product itself was capable of converting it into usable form. Having already tried inserting the log into a second install of the product, and had the same resulting problems, we had a go at ripping the data out using some fiddly manual tricks, with some success. To double-check, we re-ran the tests in a series of smaller scans, clearing out the log history in-between each, and finally got some usable results which compared closely with our initial findings. On one of the reinstalls, having gone no further than installing the product and tweaking the on-access settings, the machine crashed with a blue screen.

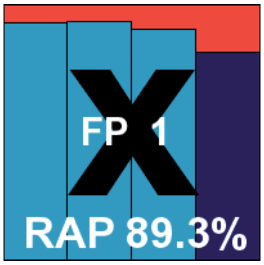
Finally putting results together, we saw the expected solid detection rates across the test sets, with the WildList and clean sets properly handled and a VB100 award just about earned. The product itself seemed far from solid though, to the extent that our initial reaching out to the developers included a query as to whether this was actually a pre-release beta build – they insisted it was a full shipping edition, but we hope that some urgent tidying up will be going on to ensure customers are not hit by as many problems as we were.

Kaspersky's history for the *I.S.* line is decent, with four passes and one fail in the last six tests, one test having been skipped; eight passes, a single fail and three tests not entered in the last two years. With several blue screens, and the product GUI crashing repeatedly under the weight of its own log data, this was one of the least stable performances this month, and despite actual testing running through in good time, the extra effort of trying to load and convert the results along with the numerous crashes and re-tests meant it took up one of our test systems for more than six full days.

Kaspersky Small Office Security 2

Version 9.1.0.59

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.55%
Worms & bots	93.84%	**False positives**	1



A slightly more familiar product, this small business edition is closer to the company's 2011 and '*PURE*' product lines. The installer is notably larger, at 214MB, and again updates were applied from a bundle mirroring a complete online update source. The install process was simple and rapid, all done in under a minute with no reboot required.

The interface is more standard than the newer edition, offering a wide range of components in a smoothly integrated fashion, and again a massively detailed level of configuration is available, in a splendidly clear format. Testing ran through with minimal effort, the product showing responsiveness and stability throughout.

Archive scanning		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 Internet Security	OD	X	√	X	X	X	√	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Avast Software avast! Free Antivirus	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
AVG Internet Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira AntiVir Personal	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
Avira AntiVir Professional	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
BitDefender Security for File Servers	OD	√	√	8/√	8/√	√	√	√	8/√	√	√	√
	OA	8/√	8/√	4/√	4/√	8/√	8/√	8/√	4/√	8/√	8/√	√
BullGuard Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	2	2	1	1	2	2	2	1	2	2	√
Central Command Vexira	OD	√	2/√	√	√	X/√	X	√	√	√	X/2	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Clearsight Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Commtouch Command Anti-Malware	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2/4	2/4	2/4	2/4	2/4	√	2/4	1/2	2/4	2/4	√
Comodo Antivirus	OD	X	2	5	5	5	5	5	2	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Comodo Internet Security PREMIUM	OD	X	2	5	5	5	5	5	2	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Defenx Security Suite 2011	OD	X	X	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Digital Defender Antivirus Pro	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
eEye Digital Security Blink Professional	OD	X	1/√	1/√	1/√	1/√	1/√	1/√	8/√	2/√	X	√
	OA	X	X/1	X/1	X/1	X/1	X/1	X/1	√	X/2	X	√

Key:
√ - Detection of EICAR test file up to ten levels of nesting
X - No detection of EICAR test file
X/√ - default settings/all files
1-9 - Detection of EICAR test file up to specified nesting level
?? - Data could not be gathered
* Detection of EICAR test file with randomly chosen file extension
(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Emsisoft Anti-Malware	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	??	??	??	??	??	??	??	??	??	??	??
eScan Internet Security Suite	OD	√	7	6	5	7	7	7	7	8	√	√
	OA	X/√	X/√	X/8	X/8	X/√	X/√	X/√	X/√	X/8	X/√	√
ESET NOD32 Antivirus	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√	√	√
Frisk F-PROT Antivirus for Windows	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	2	2	X	X	X	2	2	√
F-Secure Client Security	OD	X	5	5	5	5	5	5	2	5	X	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
G Data AntiVirus 2012	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	8/√	8/√	√	√
GFI VIPRE Antivirus	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Ikarus virus.utilities	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	2	2	2	2	2	2	2	3	2	2	√
Iolo System Shield	OD	5/√	5/√	5/√	5/√	5/√	√	5/√	2/5	5/√	5/√	√
	OA	5	5	5	5	5	√	5	2	5	5	√
Kaspersky Internet Security 2012	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky Small Office Security 2	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Lavasoft Ad-Aware Total Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	1/√	1/√	√	√	√	8/√	8/√	√	√
LogicOcean Gprotect	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
McAfee VirusScan Enterprise	OD	2	√	√	√	√	√	√	√	√	X	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/v	X/√	X	√
Microsoft Security Essentials	OD	√	√	√	√	2	2	2	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√

Key:
√ - Detection of EICAR test file up to ten levels of nesting
X - No detection of EICAR test file
X/√ - default settings/all files
1-9 - Detection of EICAR test file up to specified nesting level
?? - Data could not be gathered
* Detection of EICAR test file with randomly chosen file extension
(Please refer to text for full product names)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Norman Security Suite	OD	X	√	8	1	√	√	√	8	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
PC Booster AV Booster	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
PC Tools Internet Security	OD	√	√	√	√	√	√	√	1	√	X	X
	OA	X	X	8	√	X	X	X	X	X	X	X
PC Tools Spyware Doctor with AV	OD	4	√	√	√	√	√	√	5	√	X	X
	OA	X	X	8	√	X	X	X	X	X	X	X
Preventon	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Qihoo 360 Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Quick Heal Antivirus Pro 2011	OD	2	X/5	X	X	X/5	X	X/5	X/1	X/5	X	√
	OA	X/2	2	X	X	2	X	2	1	2	X	X/√
Returnil System Safe	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Rising Internet Security	OD	??	??	??	??	??	??	??	??	??	??	??
	OA	X	X	√	√	X	X	X	X	X	X	√
Security Coverage SecureIT 2011	OD	X/√	X/√	X/8	X/8	X/√	X	X/√	X/8	X/√	X/√	√
	OA	√	√	8	8	√	X	√	8	√	√	√
Sophos Endpoint Security & Control	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	5	5	5	5	5	5	5	5	5	√
SPAMfighter VIRUSfighter	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Total Defense Inc. ISS Plus	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	1	X	X	X	1	X	√
Total Defense Inc. Total Defense r12	OD	X	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	X/√	√
	OA	X	X	X	X	1	X	X	X	1	X	√
TrustPort Antivirus 2012	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
VirusBuster Professional	OD	√	2/√	√	√	X/√	X	√	√	√	X/2	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√

Key:
√ - Detection of EICAR test file up to ten levels of nesting
X - No detection of EICAR test file
X/√ - default settings/all files
1-9 - Detection of EICAR test file up to specified nesting level
?? - Data could not be gathered
* Detection of EICAR test file with randomly chosen file extension
(Please refer to text for full product names)

Scanning speeds were superb, with barely noticeable overheads on access, low use of CPU even when busy and RAM use low at idle and no more than average during heavy activity. Impact on our set of tasks was noticeable, but not excessive.

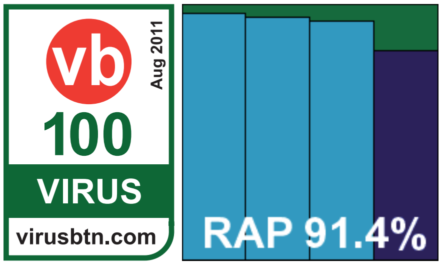
All detection tests completed in good time, with no problems converting data into a readable format, and results looked solid, with good coverage across the sets. The WildList presented no difficulties, but in the clean sets a single item, a developer tool from *Microsoft*, was alerted on as a threat, denying *Kaspersky*'s second offering a VB100 award this month despite a far more convincing performance. The developers inform us that the false alarm would have been mitigated by the company's online reputation look-up system in real-world use, but under the current test rules such systems cannot be taken into account (we plan to introduce some significant changes in the near future which will include coverage of these 'cloud' components).

For now, *Kaspersky*'s business line must take the hit, but it has a decent record, with four passes and two fails in the last six tests; eight passes, three fails and a single test not entered in the last two years. The product ran very stably throughout, comfortably completing all tests within our target time of 24 hours.

Lavasoft Ad-Aware Total Security

Ad-Aware AntiVirus version 21.1.0.28

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.74%
Worms & bots	99.43%	**False positives**	0



This month *Lavasoft* only entered its '*Total*' product, which is based around the *G Data* engine with some extras of its own; we expect to see the company's '*Pro*' product (which includes the *VIPRE* engine) appearing once again in an upcoming test. The installer for the *Total* solution is a chunky 482MB with all updates rolled in, but the set-up process is not overly long considering the size. A reboot is needed to complete, and after the restart we noted the machine took a long time to come back to life. Once up and running we saw an error message stating that *Ad-Aware* could not be loaded, apparently due to 'insufficient memory' (the test machines boast a mere 4GB of RAM, which is perhaps not as enormous these days as it was a year or two ago). After a few moments though things settled down nicely, and the product loaded up fine.

The interface is pretty similar to *G Data*'s, with only the branding noticeably different, and this means it is admirably clear and well laid out, with a wealth of options easily accessible. After the initial wobble it ran smoothly, powering through the speed tests with excellent optimization in the warm runs after a fairly sluggish first look, and a little slower when the default cap on the size of files to scan was disabled. Use of resources was not bad at all, and impact on our set of tasks was not too heavy either.

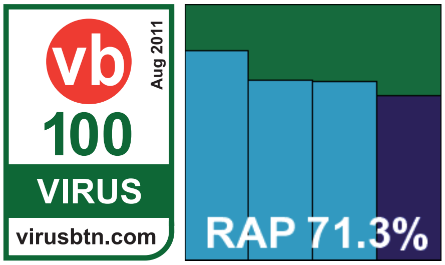
Detection rates were superb, the main sets completely blown away and the RAP sets dealt with well (although not scoring quite as well as *G Data*, hinting that perhaps the definitions provided were not quite as recent) – presumably real-world users would have an even better experience.

The clean sets were splendidly well handled, and with no problems in the WildList *Lavasoft* earns another VB100 award for the *Total* solution. Having entered four of the last seven tests, the product now has two passes and two fails, with initial teething problems apparently sorted out and a long and glorious VB100 career on the horizon. The only issue noted was the slow initial startup, which was not repeated on subsequent reboots, and from there on testing romped through in excellent time, completing in under the target 24-hour period.

LogicOcean Gprotect

Version 1.1.68, Definitions version 14.0.90

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.61%
Worms & bots	91.69%	**False positives**	0



Another from the *Preventon* stable, *Gprotect* has only one previous entry under its belt but promised few surprises for the lab team. Like others in this cluster of products, the installer weighed in at 63MB, installed in a simple and rapid manner with no need to reboot, but a web connection was needed to activate. A reasonable degree of controls were offered in a clear and simple interface. Once again logging defaulted to extreme verbosity, and dumped data older than a few busy minutes of scanning, but some tweaks to the GUI and registry easily fixed these oddities.

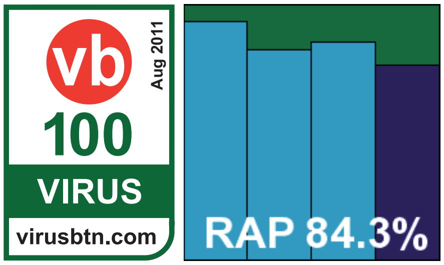
Running through the tests was untaxing, though a little uncomfortable on the eye thanks to the garish purple, green and orange colour scheme. Scanning speeds were decent, with reasonable overheads on access. Resource consumption and impact on our set of tasks were not bad either, and detection rates were solid and workmanlike, if a little less than inspiring.

The core certification sets were handled well, earning *Gprotect* its second VB100 award from its second entry in the last three tests, the middle one having been skipped. Stability was solid throughout, and testing took only slightly over the planned 24 hours to complete.

McAfee VirusScan Enterprise & AntiSpyware Enterprise 8.8

Scan engine version 5400.1158, DAT version 6383.0000

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.30%
Worms & bots	94.44%	**False positives**	0



McAfee’s corporate solution is one of few to have changed little over several years of regular testing, and remains grey and serious as befits its business target market. The installer is a smallish 37MB, accompanied by updates measuring 107MB unpacked, and sets up in reasonable time after a fair number of questions, including an offer to disable *Windows Defender*. A reboot is not demanded, but is required for some components to become fully operational.

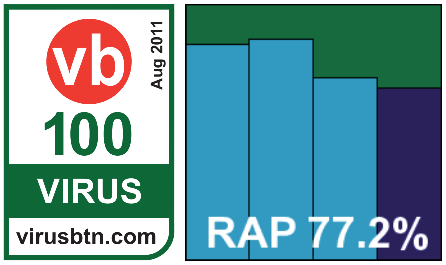
The interface is plain and simple, with an olde worlde feel to it, but is very easy to use and offers an impeccable level of fine-tuning to suit the most demanding of users. It ran very stably throughout the test period, showing some good on-demand speeds, with a little speed-up in the warm runs, and on-access overheads a shade on the high side of medium. RAM use was a little higher than most, but CPU use and impact on our set of tasks was not excessive.

Detection rates were very good in the main sets and decent in the RAP sets, with scores declining very slightly through the weeks. The core certification sets were handled perfectly, earning *McAfee* another VB100 award. The product seems to be recovering from something of a rough patch, with two passes and one fail in the last six tests, and three not entered; six passes and two fails over the past two years, with four tests skipped. No problems were observed this month, and testing completed in good time, around the one day hoped for from all products.

Microsoft Security Essentials

Product version 2.0.0657.0, Signature version 1.105.2231.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.62%
Worms & bots	95.62%	**False positives**	0



The base installer for *Microsoft*’s free-for-home-use solution was one of the smallest this month, at just 9.6MB, but updates of 64MB brought the total download required to a more standard size. The set-up process was simple and fairly speedy, with minimal user interaction, but a reboot was needed at the end. The interface is well integrated into *Windows* styling, as one would expect, and is generally usable although the language used is occasionally a little unclear. Configuration is fairly basic, but a few options are provided, and stability was firm and reliable throughout.

Scanning speeds were not the fastest but overheads were very light indeed, with minimal use of resources and only the tiniest impact on our set of tasks. Detection rates, when usable data had been pulled out of rather unfriendly logs, were good in the main sets and decent in the RAP sets too, dropping off a little into the later weeks. The core WildList and clean sets were dealt with well, and a VB100 award is duly granted to *Microsoft*.

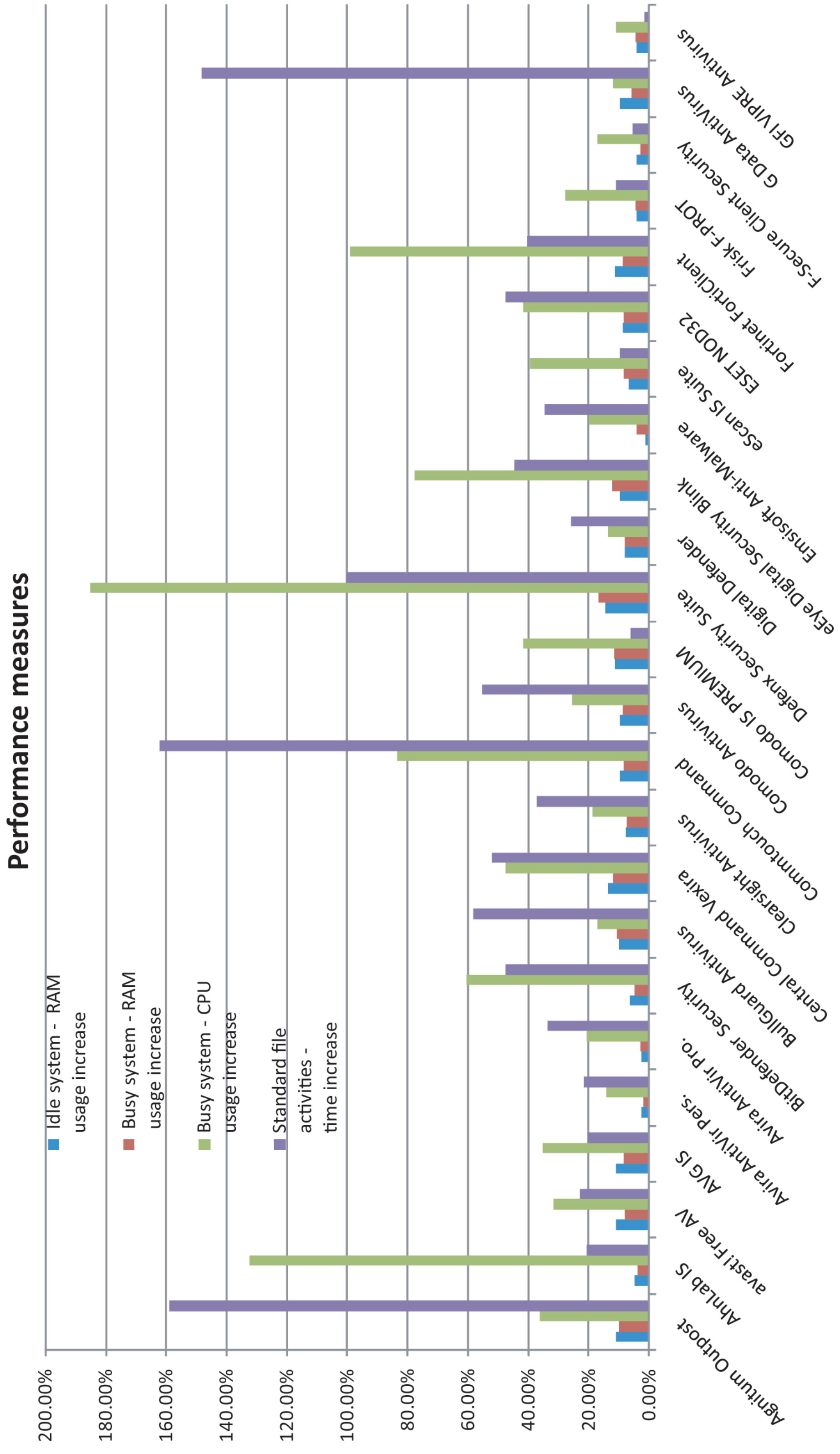
This product is usually only entered for alternate tests, with the company’s *Forefront* solution submitted for server platforms. *Security Essentials*’ history now shows two passes from two entries in the last six tests; four passes and a single fail since first appearing in December 2009.

Performance measures	Idle system - RAM usage increase	Busy system - RAM usage increase	Busy system - CPU usage increase	Standard file activities - time increase
Agnitum Outpost	11.12%	9.96%	36.39%	158.79%
AhnLab IS	4.75%	3.95%	132.49%	20.68%
Avast Software avast!	10.94%	8.02%	31.59%	22.88%
AVG Internet Security	11.09%	8.50%	35.18%	20.30%
Avira AntiVir Pers.	2.54%	1.93%	14.20%	21.56%
Avira AntiVir Pro.	2.70%	2.76%	20.67%	33.77%
BitDefender Security	6.56%	4.71%	60.64%	47.57%
BullGuard Antivirus	10.03%	10.80%	17.23%	58.23%
Central Command Vexira	13.49%	12.10%	47.62%	51.99%
Clearsight Antivirus	7.69%	7.37%	18.83%	37.19%
Commtouch Command	9.57%	8.54%	83.44%	162.15%
Comodo Antivirus	9.70%	8.87%	25.65%	55.37%
Comodo IS PREMIUM	11.47%	11.79%	41.89%	6.28%
Defenx Security Suite	14.45%	16.94%	185.07%	100.32%
Digital Defender	8.15%	8.02%	13.46%	25.74%
eEye DS Blink	9.70%	12.31%	77.75%	44.66%
Emsisoft Anti-Malware	1.19%	4.08%	20.05%	34.50%
eScan IS Suite	6.85%	8.29%	39.41%	9.87%
ESET NOD32 Antivirus	8.64%	8.43%	41.76%	47.67%
Fortinet FortiClient	11.17%	8.77%	99.17%	40.48%
Frisk F-PROT	4.17%	4.60%	27.84%	11.07%
F-Secure Client Security	4.36%	2.82%	17.03%	5.61%
G Data AntiVirus	9.70%	5.80%	11.92%	148.25%
GFI VIPRE Antivirus	4.29%	4.57%	11.12%	1.65%
Ikarus virus.utilities	6.86%	7.17%	48.28%	47.09%

Performance measures contd.	Idle system - RAM usage increase	Busy system - RAM usage increase	Busy system - CPU usage increase	Standard file activities - time increase
Iolo System Shield	33.32%	6.69%	91.16%	146.21%
Kaspersky IS 2012	4.50%	5.02%	22.25%	13.57%
Kaspersky SO Security 2	7.00%	26.23%	19.07%	62.51%
Lavasoft Ad-Aware TS	7.58%	10.80%	36.57%	55.28%
LogicOcean Gprotect	7.58%	7.45%	24.42%	23.89%
McAfee VirusScan	27.91%	27.38%	34.22%	17.84%
Microsoft SE	6.10%	5.15%	5.97%	6.28%
Norman Security Suite	6.64%	5.27%	86.69%	2.16%
PC Booster AV Booster	7.39%	7.29%	16.80%	49.35%
PC Tools IS	12.02%	9.61%	59.38%	43.87%
PC Tools SD with AV	11.51%	11.02%	55.56%	37.92%
Preventon	6.40%	6.47%	13.61%	56.99%
Qihoo 360 Antivirus	7.56%	6.12%	36.47%	5.90%
Quick Heal Antivirus Pro	31.56%	19.35%	-82.38%	2350.03%
Returnil System Safe	6.03%	5.30%	64.94%	71.81%
Rising Internet Security	3.78%	3.12%	104.14%	42.86%
Security Coverage SecureIT	7.27%	5.15%	37.51%	51.17%
Sophos ESC	6.28%	13.28%	42.81%	41.27%
SPAMfighter VIRUSfighter	6.11%	6.55%	39.86%	60.94%
Total Defense ISS Plus	18.05%	18.63%	36.92%	38.23%
Total Defense TD r12	21.17%	20.90%	80.02%	108.87%
TrustPort Antivirus 2012	9.41%	10.13%	56.78%	24.81%
VirusBuster Professional	7.46%	9.63%	36.08%	63.22%

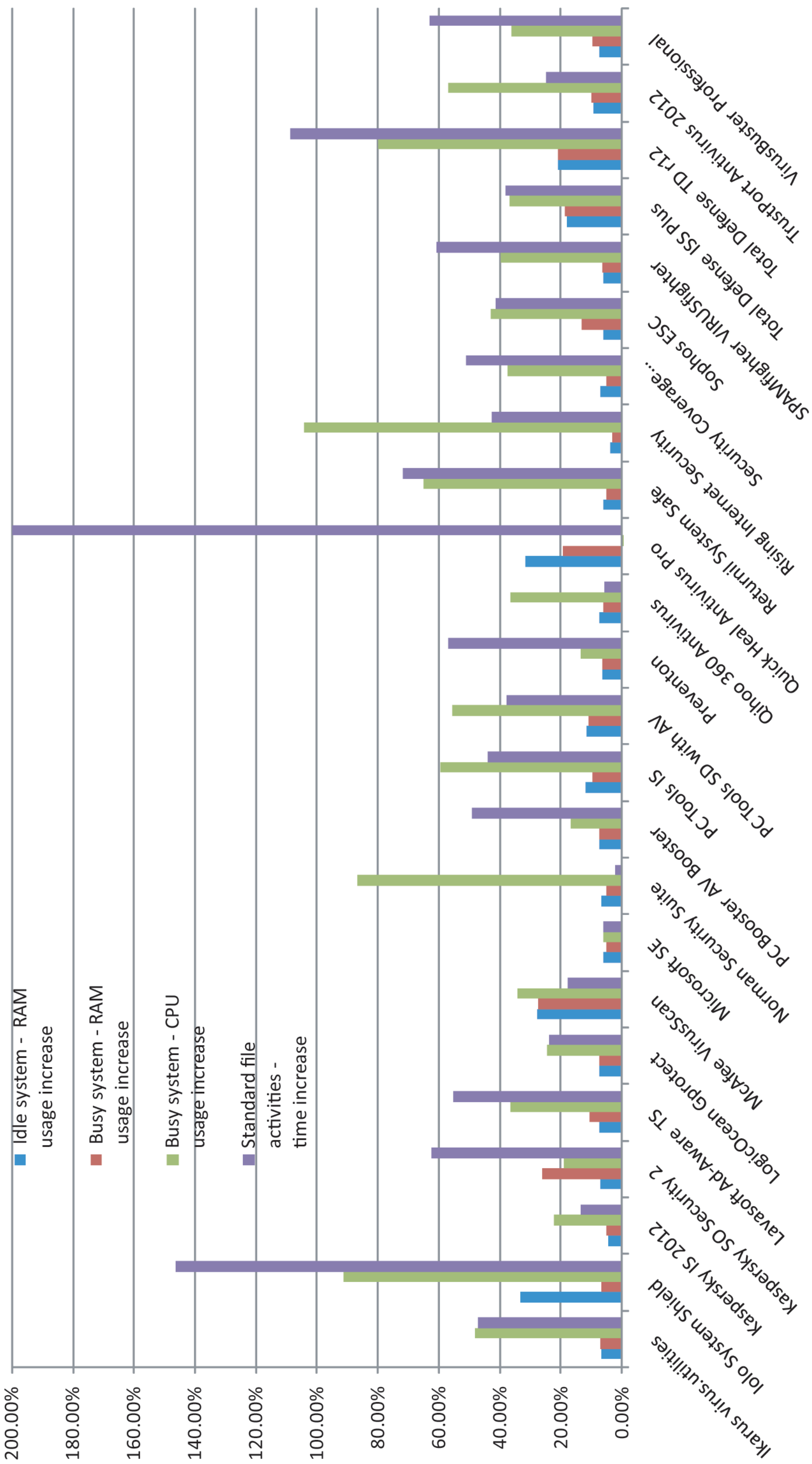
* Negative value for busy CPU due to long idle periods during measurements

(Please refer to text for full product names)



(Please refer to text for full product names)

Performance measures contd.



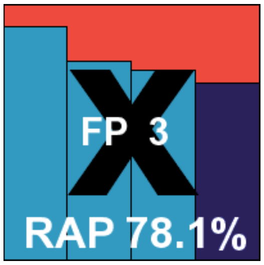
(Some values exceed chart area)

(Please refer to text for full product names)

Norman Security Suite

Antivirus version 8.00, Norman scanner engine version 6.07.10

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	94.22%
Worms & bots	93.19%	**False positives**	3



Norman's suite solution has raised some eyebrows in the past with the occasional moment of eccentricity, and we looked forward to more surprises this month. The 135MB installer ran through surprisingly quickly, with only a few steps to click through, but ended with a request to reboot.

The interface remains quirky and occasionally flaky, with the status page frequently warning that anti-malware components are not installed despite them clearly being fully operational. Scanning speeds were as slow as ever thanks to the in-depth sandboxing system, and on-access overheads were heavy too. Use of CPU cycles when busy was pretty high, but memory use and impact on our set of tasks were surprisingly low.

Getting through our large infected sets took some time, but not excessively long, and results showed some pretty decent scores in the main sets, with a reasonable showing in the RAP sets too. In the clean sets however (and as expected, given the results of other products using the same engine), a number of items were labelled as malware, and *Norman* does not quite make the grade for a VB100 award this month.

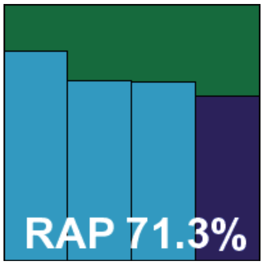
The vendor's recent history is good, with five passes and just this one fail over the last six tests; longer term things look a little more rocky, with five passes and five fails in the last two years, two tests having been skipped. Other than the occasional odd message from the GUI, stability was mostly pretty good this month, and having been carefully scheduled to run over a weekend, testing only took up two full days of live lab time.

PC Booster AV Booster

Version 1.1.68, Definitions version 14.0.90

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.61%
Worms & bots	91.69%	**False positives**	0

Another member of the *Preventon* clan, with two previous appearances in our tests, *AV Booster* followed the familiar pattern of a 63MB installer, which was quick to run but needed web access to function and to apply a licence code at the end. No reboot was needed. Operating the simple, minimal GUI was straightforward, and tests ran through smoothly.



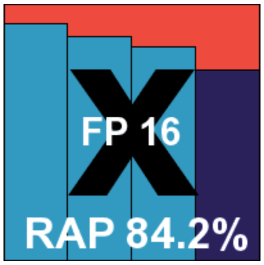
Scanning speeds were OK, overheads a little lighter than average, with reasonable resource use and an unintrusive effect on our set of activities. Scores were generally decent too, tailing off through the RAP sets as expected. No problems in the WildList or clean sets mean a VB100 award is earned by *PC Booster*, giving the vendor two passes and one fail in the five tests since its first appearance.

Stability was good with no freezes, crashes or other problems, although the product's verbose logging was a little strange. With decent speeds in the larger sets, all tests were completed in only just over the 24-hour target limit.

PC Tools Internet Security

Version 2011 (8.0.0.654), Database version 6.17760

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.72%
Worms & bots	96.39%	**False positives**	16



As usual a brace of products was submitted by *PC Tools*, now a subsidiary of the mighty *Symantec*, whose own product is absent from this month's test. This version of *PC Tools* includes a firewall and other components on top of the standard malware protection, and the installer is a fair size at 216MB, including all updates. The set-up process has only a few dialogs but takes several minutes to complete, with no reboot needed to finish off.

The interface hasn't changed much in the few years since we first encountered this range, but it doesn't look too dated. The design more or less follows standard practice, but configuration is pretty sparse in places, and where there are options they are often less than clear. Operation proved reasonably straightforward though, and the tests ran through without too much difficulty.

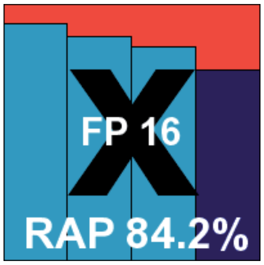
Scanning speeds were pretty good, with some splendid optimization in the warm runs, and on-access overheads were very light. Use of system resources was perhaps a little above average, but our set of activities were completed in decent time. The scanning of the main sets took rather longer than we would have hoped, but completed without any problems, showing some very solid scores across the sets. The WildList caused no problems, but in the clean sets a number of items were alerted on as 'Zero.Day.Threat', including some components from a major business package from *IBM*. This spoiled *PC Tools*' chances of a VB100 award this month.

The suite's history is good, with entries only on desktop platforms resulting in two passes and now a single fail in the last six tests, with three tests skipped; five passes and a fail from six entries in the last two years. No crashes or stability issues were encountered, but slow handling of our large test sets meant that testing took around 48 hours to complete.

PC Tools Spyware Doctor with AntiVirus

Version 8.0.0.624, Database version 6.17760

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	94.72%
Worms & bots	96.39%	**False positives**	16



The *Spyware Doctor* brand has a long history, and again the current version is much the same as those we have seen over the past few years. The installer weighed in at 197MB – slightly smaller than its suite counterpart thanks to a slightly smaller range of components, and the install process was a little quicker, completing in a couple of minutes with again no need to reboot.

The GUI is bright and shiny, with lots of status information on the front page and settings sections for a wide range of sub-components. For the most part, however, these controls are limited to 'on' or 'off', with little fine-tuning available. Usage was not too difficult though, and the tests ran through without problems.

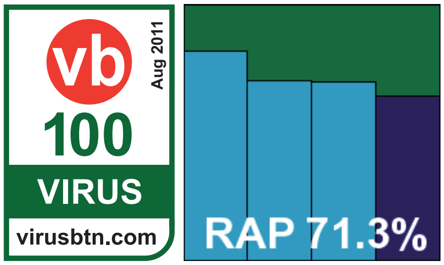
Scanning speeds were impressive and overheads very light, especially on the warm runs. Use of resources was around average, with a middling hit on our set of tasks. Good detection rates extended across all sets, drifting downwards into the later weeks of the RAP sets, and the WildList was covered flawlessly. As feared though, the same handful of false alarms – clearly caused by over-sensitive heuristics – cropped up in the clean sets, denying the product certification this month.

The product's history again reflects the pattern of desktop comparatives alternating with server platforms, with two passes and a fail from three entries in the last six; five passes and this one fail in the last two years, with all six server tests skipped. Stability was generally sound throughout, although the on-access run over our infected sets did have to be repeated when it appeared the protection had simply switched off halfway through the first attempt. Obtaining a full set of results thus took close to three full days of testing.

Preventon

Version 4.3.68, Definitions version 14.0.90

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.61%
Worms & bots	91.69%	**False positives**	0



The source of a number of this month's products, and itself based on the *VirusBuster* engine, *Preventon* closely followed an already well established pattern. The 64MB installer set things up quickly, with no reboot, and after some tweaks to the simple settings and some registry changes to allow reliable logging, tests ran through pleasantly smoothly. Speeds and resource usage were on the good side of average, with only the suite of activities taking a little longer than expected.

Detection rates were not bad in the main sets, less than stellar in the RAPs but still respectable, and with no problems in the core certification sets a VB100 award is comfortably earned. *Preventon*'s history is slightly longer than many of its partners, showing three passes and a single fail in the last six tests, with two not entered; five passes and two fails in the last two years. No issues were noted during testing, which took just a little longer than the target 24 hours to complete.

Qihoo 360 Antivirus

App version 2.0.0.2033, Signature date 2001-06-20

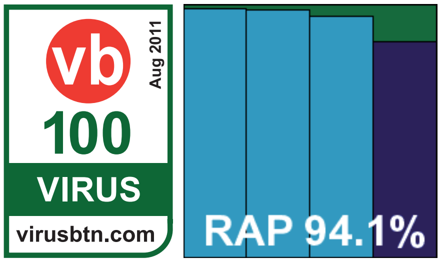
ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.57%
Worms & bots	99.64%	**False positives**	0

Reactive And Proactive (RAP) scores	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Agnitum Outpost	VIRUS 100	86.18%	81.42%	75.04%	80.88%	67.99%	77.66%
AhnLab Internet Security		90.85%	84.31%	81.39%	85.52%	71.10%	81.91%
Avast Software avast! Free Antivirus	VIRUS 100	97.83%	97.80%	93.45%	96.36%	81.68%	92.69%
AVG Internet Security		95.60%	95.83%	92.34%	94.59%	76.37%	90.03%
Avira AntiVir Personal	VIRUS 100	97.84%	95.77%	93.83%	95.81%	85.43%	93.22%
Avira AntiVir Professional	VIRUS 100	97.84%	95.77%	93.83%	95.81%	85.43%	93.22%
BitDefender Security for File Servers	VIRUS 100	95.11%	92.91%	93.81%	93.94%	81.92%	90.94%
BullGuard Antivirus	VIRUS 100	98.25%	97.69%	96.97%	97.64%	86.55%	94.87%
Central Command Vexira	VIRUS 100	86.20%	81.47%	74.93%	80.87%	67.92%	77.63%
Clearsight Antivirus	VIRUS 100	81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
Commtouch Command Anti-Malware	VIRUS 100	70.89%	61.99%	66.21%	66.36%	66.72%	66.45%
Comodo Antivirus		90.55%	66.32%	64.51%	73.79%	46.65%	67.01%
Comodo Internet Security PREMIUM		90.55%	66.32%	64.51%	73.79%	46.65%	67.01%
Defenx Security Suite 2011	VIRUS 100	85.80%	76.26%	72.47%	78.17%	67.78%	75.57%
Digital Defender Antivirus Pro	VIRUS 100	81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
eEye Digital Security Blink Professional		91.19%	77.46%	74.25%	80.97%	69.13%	78.01%
Emsisoft Anti-Malware		99.66%	99.39%	96.84%	98.63%	84.68%	95.14%
eScan Internet Security Suite	VIRUS 100	98.23%	97.64%	95.82%	97.23%	85.35%	94.26%
ESET NOD32 Antivirus	VIRUS 100	90.82%	91.58%	93.25%	91.88%	83.24%	89.72%
Fortinet FortiClient	VIRUS 100	96.34%	93.82%	92.45%	94.20%	79.63%	90.56%
Frisk F-PROT Antivirus for Windows	VIRUS 100	69.89%	61.54%	65.52%	65.65%	65.81%	65.69%
F-Secure Client Security	VIRUS 100	77.53%	72.57%	76.57%	75.56%	68.99%	73.91%
G Data AntiVirus 2012	VIRUS 100	99.70%	99.71%	95.54%	98.32%	88.46%	95.85%
GFI VIPRE Antivirus	VIRUS 100	96.83%	95.77%	91.89%	94.83%	79.03%	90.88%

(Please refer to text for full product names)

Reactive And Proactive (RAP) scores contd.	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Ikarus virus.utilities		99.60%	99.31%	96.68%	98.53%	84.42%	95.00%
Iolo System Shield	VIRUS 100	63.83%	56.18%	60.65%	60.22%	58.42%	59.77%
Kaspersky Internet Security 2012	VIRUS 100	92.66%	92.84%	89.50%	91.67%	80.65%	88.91%
Kaspersky Small Office Security 2		92.87%	93.28%	89.96%	92.04%	81.14%	89.31%
Lavasoft Ad-Aware Total Security	VIRUS 100	96.39%	94.59%	93.02%	94.66%	81.53%	91.38%
LogicOcean Gprotect	VIRUS 100	81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
McAfee VirusScan Enterprise	VIRUS 100	93.46%	82.30%	85.15%	86.97%	76.16%	84.27%
Microsoft Security Essentials	VIRUS 100	84.38%	85.95%	71.19%	80.51%	67.26%	77.19%
Norman Security Suite		91.27%	77.55%	74.30%	81.04%	69.17%	78.07%
PC Booster AV Booster	VIRUS 100	81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
PC Tools Internet Security		92.11%	87.18%	83.03%	87.44%	74.33%	84.16%
PC Tools Spyware Doctor with AntiVirus		92.12%	87.40%	83.04%	87.52%	74.34%	84.22%
Preventon	VIRUS 100	81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
Qihoo 360 Antivirus	VIRUS 100	98.31%	97.65%	95.05%	97.01%	85.20%	94.06%
Quick Heal Antivirus Pro 2011	VIRUS 100	78.64%	55.75%	70.04%	68.14%	58.13%	65.64%
Returnil System Safe	VIRUS 100	70.74%	62.23%	66.40%	66.45%	66.76%	66.53%
Rising Internet Security	VIRUS 100	47.04%	42.85%	37.65%	42.51%	39.40%	41.73%
Security Coverage SecureIT 2011	VIRUS 100	95.34%	93.02%	94.71%	94.36%	86.76%	92.46%
Sophos Endpoint Security and Control	VIRUS 100	86.72%	85.60%	83.31%	85.21%	75.44%	82.77%
SPAMfighter VIRUSfighter	VIRUS 100	79.20%	63.21%	64.37%	68.93%	62.48%	67.32%
Total Defense Inc. Internet Security Suite Plus	VIRUS 100	80.56%	70.99%	64.10%	71.88%	59.30%	68.74%
Total Defense Inc. Total Defense r12	VIRUS 100	77.34%	67.15%	60.62%	68.37%	56.87%	65.49%
TrustPort Antivirus 2012	VIRUS 100	99.82%	99.71%	99.30%	99.61%	88.14%	96.74%
VirusBuster Professional	VIRUS 100	86.19%	81.47%	74.92%	80.86%	67.92%	77.62%

(Please refer to text for full product names)



Qihoo's product is a little quirky in its implementation, but with the *BitDefender* engine under the covers we usually manage to coax a decent showing out of it. The installer measured 122MB, including all required updates, and installed rapidly with little fuss and no need for a reboot. The interface is tidy and simple, providing a fair degree of fine-tuning, and is mostly easy to use, although language translation is a little uneven in places.

Scanning speeds were only medium, but overheads pretty light, and use of resources and impact on our set of activities were impressively low too. This may in part be down to one of the oddities of implementation in this product, which became particularly clear when running the on-access test over infected sets. I hesitate to say that the product doesn't work *properly*, the case perhaps being more that it functions *differently* from expected norms. When a detection occurs on access, be it on read or on write, access to the file is not always prevented; instead, in most cases the product simply produces a pop-up claiming to have blocked access (this could, of course, be another translation oddity). When multiple detections occur in close proximity, these pop-ups can take several hours to appear, rendering the protection much less secure than it suggests. Log entries suffer a similar delay, showing that the problem is with the detections themselves, rather than merely the pop-up system.

However, as our rules do not insist on blocking access, only on recording detections in logs, it just about scrapes by, showing some solid scores in the main sets when the logs were eventually populated. Moving on to the on-demand tests, we hit another snag when it became clear that logging was once again not being written out to file, but instead accumulating in memory, and again no sort of checking was in place to ensure that excessive amounts of RAM were not being consumed. After a couple of days' run time, with the system steadily getting slower and slower and close to 2GB of memory taken up by the scanner process, the job crashed, leaving no salvageable data for us to use. Instead we had to start from scratch, running multiple smaller jobs once more.

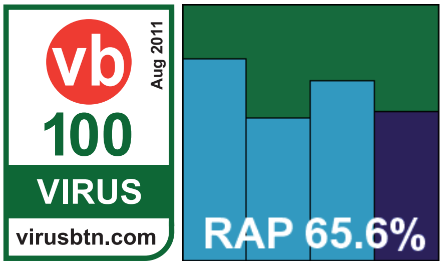
With full results finally in, the excellent scores expected from the *BitDefender* engine were recorded, with very good coverage across the sets. A VB100 award is just about granted, although it does seem that 'not working properly' is not so very far from the truth. *Qihoo* has managed to scrape four passes from the last six tests, with two not entered, and in the ten tests since its first appearance shows six passes and a single fail, with three no-entries.

Stability was shaky at best, with a very unconvincing approach to on-access protection and some crazy swamping of memory during large scans, causing nasty crashes of the product and serious slowdown of the test system. With multiple re-runs required, testing consumed more than five days of lab time.

Quick Heal Antivirus Pro 2011

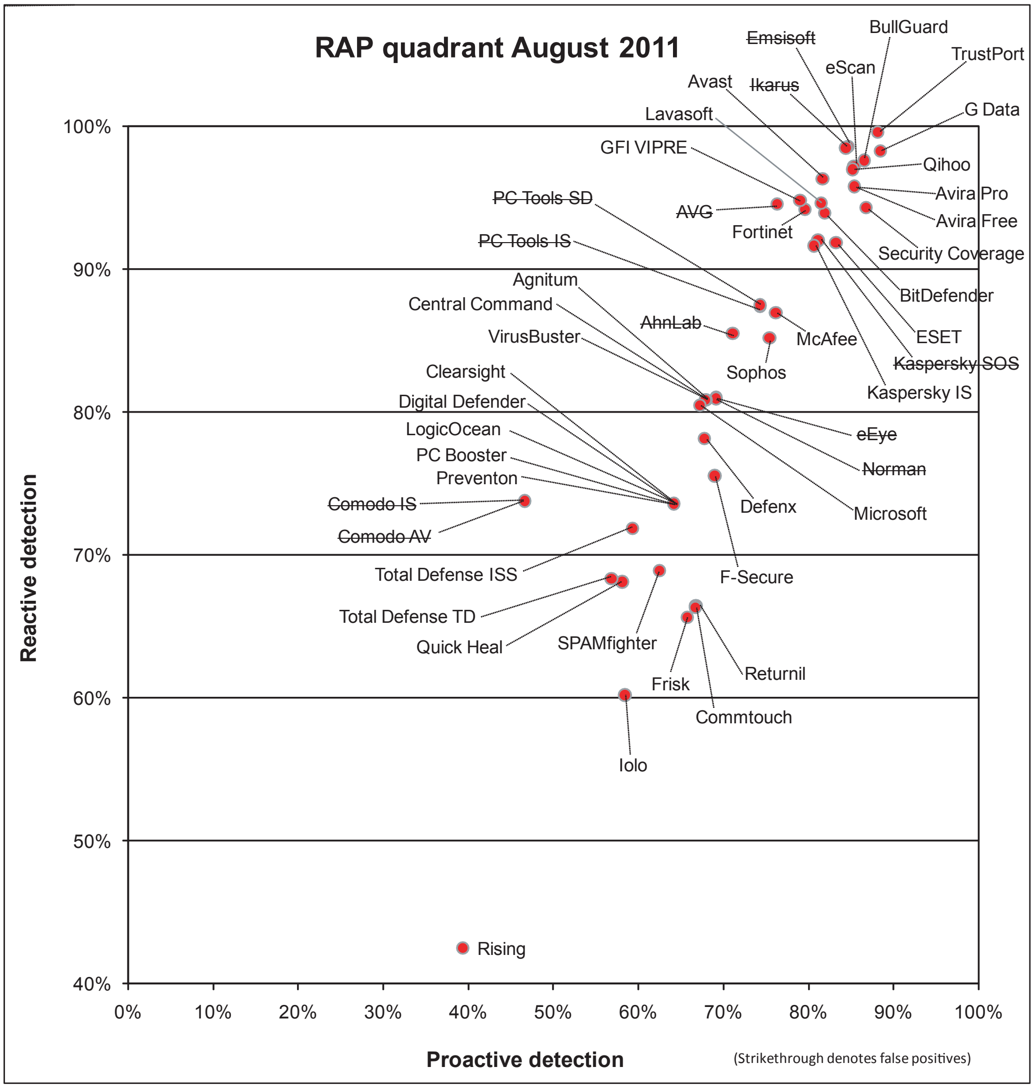
Version 12.00 (5.0.0.6), SP1

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.99%
Worms & bots	90.77%	**False positives**	0



Another of our most senior and regular participants, *Quick Heal*'s 2011 product was provided as a fairly large 210MB package including latest updates. The set-up process is very fast and simple though, with only a couple of clicks required and no reboot. The interface is hot red in colour, and is fairly user-friendly with a reasonable layout, although the configuration system can sometimes be confusing. A decent, if not quite comprehensive range of controls are provided.

Scanning speeds were not bad, and overheads pretty light too in the simple file-access tests, but in our activities test things took a turn for the weird. With fairly high RAM use both when idle and during busy times, our measure of CPU was totally thrown off balance, with a figure that was considerably lower than the baselines taken on unprotected systems. The reason for this is apparent, as running through our activities took an enormously long time to complete; with CPU use being measured periodically throughout the activities, it appears that rather than rushing through and remaining busy throughout, as is the case with the baselines and all other products, here the system spent long periods completely idle. We have already had some discussions as to the cause of this with the developers, after seeing a similar oddity in the last test, but as yet no clear reason has been provided. It seems likely, however, that some sort of URL checking is being attempted during the file download stages, but as the URL being fetched from is on an internal intranet, the product simply waits a long time for results before giving up and allowing the downloads to continue.



Moving on to the detection tests, these zipped through in much better time, showing some pretty reasonable scores, noticeably better on demand than on access and with an unusual irregularity in the RAP sets. The core certification sets were well dealt with, earning *Quick Heal* a VB100 award without difficulty.

The vendor's record is very good indeed, with six passes in the last six tests; 11 out of 12 with a single fail in the last two years. No stability issues were observed, and the slowdown in the activities measures seems likely to be due to the lack of a genuine web connection – we plan to adjust the format of this and many of our tests in the near future to avoid such oddities.

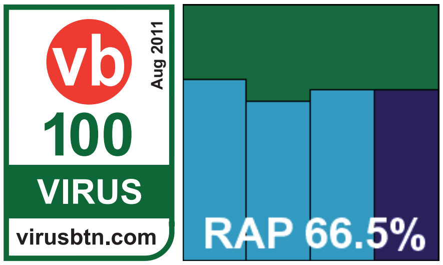
Even with the slow run time of these measures, excellent speeds elsewhere meant that all tests completed within the target time of 24 hours.

Returnil System Safe 2011

Version 3.2.12471.5765-REL13

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	80.40%
Worms & bots	75.18%	**False positives**	0

A relatively recent arrival on our radar, *Returnil* has quickly become a regular participant in our tests, combining malware detection courtesy of *Frisk* with its own unusual and intriguing virtualization and rollback system. The product remains compact though, with a 38MB installer and 28MB update bundle, and is fairly simple to set up, taking two or three minutes and needing a reboot to complete.



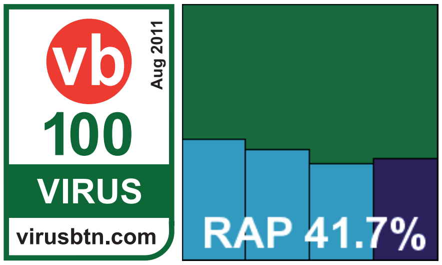
The interface is slick and attractive, with minimal configuration provided, but a simple and clear layout make it almost impossible to get lost. Scanning speeds were on the slow side, and overheads fairly heavy in the on-access measures, with CPU use fairly high too, although RAM use was pretty low. Impact on our set of tasks was also a little on the high side.

Detection rates were somewhat mediocre, but far from the worst seen this month, and the core sets presented no difficulties, earning *Returnil* a VB100 award without much difficulty. The vendor's history shows four passes and two fails in the seven tests since its first appearance, only the annual *Linux* test having been skipped. Stability proved solid throughout testing, and with no serious delays everything was dealt with in just over a day.

Rising Internet Security

Version no. 23.00.35.68

ItW	100.00%	**Polymorphic**	99.95%
ItW (o/a)	100.00%	**Trojans**	33.56%
Worms & bots	24.59%	**False positives**	0



Rising is perhaps one of China's best-known anti-malware firms, but its showings in our tests have been sporadic and unpredictable. The latest product version is new to us, and we started work on the 88MB installer with some interest. The set-up process was fairly standard, running through a fair number of stages taking several minutes to complete; at one point a pop-up warned that network connection would be interrupted briefly, but no reboot was needed to complete.

The interface is rather unusual, decorated with a swirly star-scape background reminiscent of the set of a 1980s TV game show, while the front page is dominated by graphs and charts of activity and detections. There are a number of configuration screens seemingly offering quite a lot of control, but some poor translation renders much of it almost unusable without resorting to guesswork and trial-and-error. Stability seemed reasonable, although there was an occasional wobble in the interface. Speed tests ran through without problems, showing some OK scanning speeds and overheads a little higher than we like to see. RAM use was low and CPU use rather high, while our set of tasks took an average hit – noticeably slower than the baseline measures but not too much so.

Detection tests were a little trickier to perform, as the on-access controls lacked options to fully block access on detection. Instead we resorted to trying to clean up – always a much slower process. The protection seemed a little flaky too, with several scan attempts producing slightly different results each time. On-demand tests were even trickier, as scans frequently aborted unexpectedly, or ran to completion showing numerous detections as they went, only to present a screen declaring that nothing had been found. Logs proved this not to be the case, but were capped at an unpredictable length, meaning that tests had to be run multiple times to gather full data, and even then it was not clear that some detections had been dropped from the logging system. An 'export' button was available in the logging system, but this was perpetually greyed out, and there seemed to be no way of displaying the log data in the interface, other than in the form of some graphs and statistics.

Results were eventually compiled though, showing what at first seemed to be a large number of false alarms, but closer analysis showed these were all labelled merely 'suspicious' (as were a fair few genuinely malicious items, which could not be counted as detections). The WildList was properly handled though, and with no full false alarms in the clean sets, *Rising* just about makes the grade for a VB100 award.

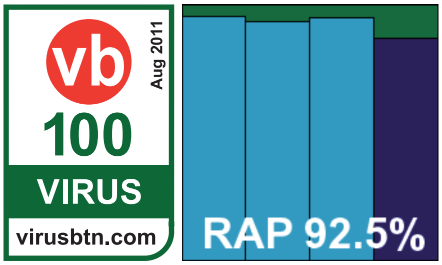
This is only the company's second entry in the last six tests, giving it one pass and one fail; over two years, it now has three passes and two fails from five attempts. There were quite a few issues with the product, including misleading information and unexpected loss of log data, as well as uneven results from on-access tests. The missing data and the need for many re-runs meant the product needed several installs and took nearly eight days of machine time, upsetting our schedule somewhat.

Security Coverage SecureIT 2011

Product version 20110610

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.21%
Worms & bots	98.85%	**False positives**	0

Not entirely a newcomer, the name of *Security Coverage* has appeared once before in our tests, but that was more than three years ago and with a very different product. The current one uses the *BitDefender* engine, as have many this



month, and was provided as a 36MB install package, with online updating required. The initial welcome screen looked very professional, and the set-up process included the option of a 'fresh start' install, which would involve the company's techs cleaning up the target system prior to installing the product. We opted for the manual route, and the rest of the set-up zipped through in good time, the whole job completing in under a minute, with no need to restart. The online update that followed was a very different experience though, with 113MB of data pulled down very slowly, taking almost an hour to complete.

When we finally got to have a look at it, the interface was attractive and clear, following a standard approach to layout and presenting a good range of controls in an easily accessible style. Initial tests ran through nicely, gathering some impressively fast scanning speeds and very reasonable overheads on access. Scanning the system drive proved a little tricky though, as the scan appeared to get stuck part way through; some investigation showed that this was an interface problem, the scan having reached an end some time ago but the GUI having failed to register anything after a certain point. This problem recurred several times during further testing. Our resource usage measures showed nothing out of the ordinary, with RAM use on the low side and CPU use and impact on our set of tasks fairly average.

Running our larger scan jobs brought up more problems, with the clean sets waded through at a very slow pace, the GUI not registering any progress. The system almost ground to a halt, responding only very, very slowly to any attempt to do anything; although RAM use seemed reasonable, the process was using a great deal of processor time, and the machine could not be restarted without cutting the power.

We eventually got on to other tests, and in the on-access run through our infected sets we were hit with a blue screen. After labouring through all the required tasks, monitoring logs to tell when things were finished, we finally gathered all the information needed. Logging was very verbose, including mentioning every item analysed, but showed no signs of the all-too-common practice of dumping data after some trifling level was reached. In this case perhaps some degree of caution might be sensible however – while we freely criticize products that think 4MB is too much space to use up on a modern machine, some users may feel that over 6GB of log files is a little excessive.

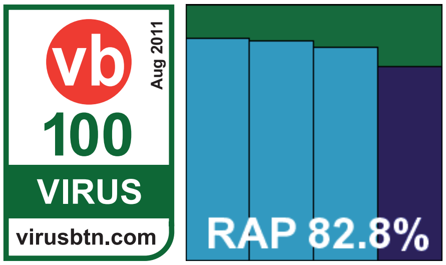
Ripping out the data needed, we found detection levels as excellent as we would expect from the engine underlying things, with splendid coverage across the sets. No problems emerged in the core sets and a VB100 award is duly earned, but the developers clearly need to a do a little more work refining things before this product is really ready.

This was *Security Coverage*'s first appearance in our tests in the last two years, so this single pass is the only record in the vendor's recent history. Testing was fraught with issues including blue screens, GUI problems, system instability and freezes including complete failure to respond, and a decidedly unusual approach to logging – in all, over six full days of lab time were taken up.

Sophos Endpoint Security and Control

Version 9.7, Sophos Anti-Virus 9.7.2, Detection engine 3.20.2, Detection data 4.66G

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.56%
Worms & bots	95.39%	**False positives**	0



Returning to more familiar territory, *Sophos* rarely misses a VB100 comparative, its last absence having been back in 2006. The current product came as an 86MB install package with a lightweight 3.5MB of incremental updates. The set-up process runs through quite a few stages but isn't too slow, completing in a few minutes with no need to reboot.

The interface is crisp and businesslike, fitting the company's corporate focus, and provides good configuration in the main control areas, with a great deal of detail available to the more adventurous admin. Navigation is generally good and clear.

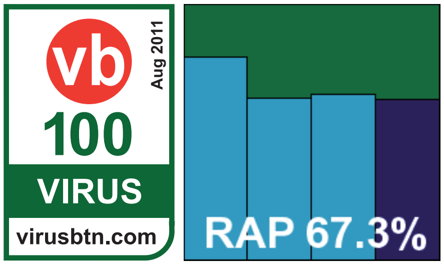
Speed tests showed some reasonable times, slower when dealing with archives, and resource usage and impact on our set of tasks were around average. A few problems were observed running through the detection tests, with scans snagging and coming to a halt several times, especially in the RAP sets. At one point the product crashed out with an error message warning that it could not connect to its service. Splitting tests into smaller chunks eventually got us through to the end though.

Detections rates were solid in the main sets, a little below our expectations in the RAP sets, but with no problems in the WildList or clean sets a VB100 award is comfortably earned. The vendor's recent history is splendid, with six passes in the last six tests; 11 in the last two years with a single fail. A few issues cropped up during testing, mainly related to handling unusually large quantities of malware, and this meant testing took around three days to complete.

SPAMfighter VIRUSfighter

Version 7.0.242

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.31%
Worms & bots	91.31%	**False positives**	0



Yet another from the *Preventon* production line, but one which at least injects a little of its own personality, *SPAMfighter* has been a regular participant in our tests for a couple of years now. The submission this month was the expected 63MB, and was set up in good time following half a dozen clicks, with no need to restart. The interface is colourful and fairly well laid out, with a reasonable level of control, although here the verbose logging mode cannot be turned off. A registry key was found which did this for us, but sadly the expected control over the log caps was absent. Checking with the developers, we were informed in no uncertain terms that old log data was never thrown out, but our experiences proved otherwise, with only a few MB of data retained at any given time. This meant the arduous task of running multiple small scans instead of leaving things running overnight, but stability proved good and the work did not take too long.

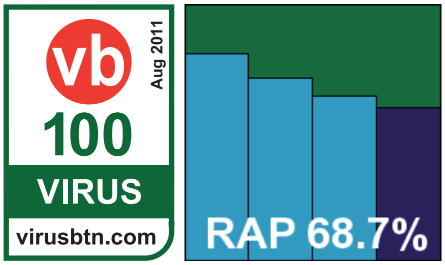
Speed measures showed reasonable throughput and not too heavy overheads, with average resource use and impact on our set of tasks leaning towards the high side. Detection rates were OK but not great – somewhat lower than other similar products, presumably down to slightly older definitions being used in this submission. No problems were encountered in the core certification sets though, and *SPAMfighter* earns another VB100 award.

This gives the product its third pass from four attempts in the last six tests, the two-year view showing four passes and three fails. Stability was generally good, but the inability to retain log data meant testing was more hands-on than usual, running to around two-and-a-half days in total.

Total Defense Inc. Internet Security Suite Plus

Security Center version 7.0.0.115, AM SDK version 1.4.1.1512, Signature file version 4399.0.0.0

ItW	100.00%	**Polymorphic**	99.96%
ItW (o/a)	100.00%	**Trojans**	85.90%
Worms & bots	88.18%	**False positives**	0



Total Defense may be an unfamiliar name, but this is a product that is well known to us. *CA*, formerly *Computer Associates*, whose products included technology brought in from companies including *Cybec* (*VET*) and *Cheyenne* (*InocuLAN*), announced plans to sell its anti-malware division some months ago, and a new firm, *Total Defense Inc.*, was formed to take over the operation of the products. Much of the development has been handled for some time now by outsourcing giant *HCL*, giving the solutions one of the most complex genealogies in a highly convoluted market space.

The home-user product, *ISS+*, remains unchanged from many recent entries, complete with *CA* branding still intact. The install package was a fairly hefty 154MB, with the submitters requesting installation and online updates on the deadline day. This process was bright and colourful, with a large 'Start' button serving both to initiate the process and to indicate acceptance of the product EULA, which is not displayed to the user by default. The set-up is accompanied by an informative slideshow, followed by a quick scan, and took three or four minutes. After this came the online update stage, which pulled down an additional 80MB of data and took a further ten minutes; a *Yahoo!* toolbar is also offered as part of the process. Finally, a reboot was needed.

The interface has become familiar through much use, but remains somewhat confusing in places thanks in part to its over-designed styling and lack of adherence to standard approaches. There is also some confusing and inconsistent use of language, but as it offers only minimal controls little actual operation was required. Speed tests tripped through with their usual alacrity, showing excellent speed-ups in the warm measures in both modes. On-access overheads were a little on the heavy side initially, but again sped up massively on re-runs. Memory use was rather higher than most, but CPU use was around average, and impact on our set of tasks was not excessive.

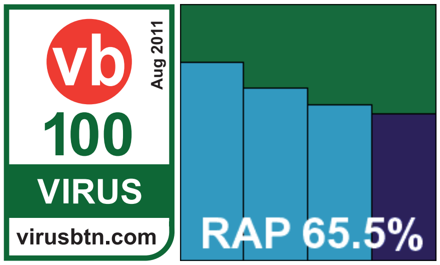
Detection tests were as labour-intensive as ever, thanks to the use of the log-to-memory approach; past experience has taught us that running large jobs overnight leads to extreme slowdowns and heavy memory usage, so multiple small jobs had to be run instead. On-access measures were easier though, as things remained light and stable even under heavy pressure.

Results showed some reasonable scores in the main sets, with RAP scores uninspiring to start with and declining steadily through the weeks. The core requirements were met though, with no misses in the WildList set and no problems in the clean sets either, and *Total Defense Inc.* earns its first VB100 award. The product itself maintains its past history, having been entered in our desktop tests (only) for the last few years; it now has two passes and one fail from three entries in the last six tests; three passes and three fails in the last two years. With the additional hands-on work imposed by the inability to handle large jobs, testing took close to 48 hours to complete, but no stability or other issues were noted.

Total Defense Inc. Total Defense r12

Product version 12.0.528, Anti-malware engine 1.5.0.1716, Anti-malware signatures 4399.0.0.0

ItW	100.00%	**Polymorphic**	99.33%
ItW (o/a)	100.00%	**Trojans**	72.79%
Worms & bots	84.25%	**False positives**	0



This month's second product from *Total Defense Inc.*, formerly developed by *CA*, is the business version which saw a major overhaul not long ago, much to the delight of the *VB* lab team at the time. However, experience quickly taught us that change is not always for the better, with the new version causing all manner of headaches and horrors. Luckily the developers saw fit to let us know this month that the client product can be installed directly from a sub-folder of the install DVD, without having to go through the painful process of setting up the management server on a separate system as we have done in previous tests, thus saving much time and effort on the busy deadline day.

We were kept fairly busy though, with the install process still far from straightforward. After running through the standard steps of accepting a EULA and so on, skipping steps relating to management servers and waiting through the two minutes or so needed to run the actual install, a reboot was needed to complete the first stage. On restarting, activation involved filling in some lengthy forms and entering a licence key received via email into boxes which refused to accept pasting, only to have it rejected for unexplained reasons. Updating then proceeded, downloading 88MB of data and taking around 15 minutes.

We then followed our normal procedure of rebooting, checking the product was operational by running some basic tests with the EICAR test file, then booting to a *Linux* platform and taking snapshots of the test system. On restoring the image later, at first all seemed fine, with the on-demand tests running through without problems; speeds were good, with excellent use of optimization, and the detection tests were once again run in small chunks thanks to the product's profligate use of memory when running large scans.

Moving on to the performance and on-access tests, some severe and immediate problems were noted. Our standard approach in running comparatives on platforms with User Access Control is to leave the controls in place in the test system images, to observe how intrusive the pop-ups are when installing and operating the products, but to disable them when running the actual tests to ease things along. This requires a reboot in *Vista*, so we restarted the test machine, only to find that it got no further than the login screen. After entering the user password, the screen went dark and stayed that way. Assuming some one-off bug, we restored the image, checked it was working, and rebooted again. Again, only a black screen. Leaving it overnight proved a little better, with some of the desktop eventually appearing, but even after a weekend the machine was not responding to any sort of input. Trying to run the test without a reboot showed the on-access component, while apparently working sometimes, was extremely unstable, shutting down for long periods without any sort of indication to the user that anything was wrong.

On contacting the developers, we found that these were in fact known problems with the product with certain versions of the real-time drivers. Apparently the update we had run had failed to complete properly, leaving us with the drivers on the original install media. Replacing these with the proper ones was not complicated thanks to our saved image, but it would presumably be more difficult for those users whose systems are essentially bricked by the product. Real-time tests then proceeded without difficulties, with all functions fully operational, and showed some heavy initial overheads, speeding up greatly in the warm measures, and fairly high use of memory and processor cycles and high impact on our suite of activities.

Processing results was a little tricky, as some of the on-demand logs proved slightly corrupted and scans had to be re-run, despite our earlier efforts. Eventually, however, a full set of figures were put together, showing scores similar to the consumer version – reasonable, but nothing to write home about. The WildList was fully covered, and no false positives emerged in the clean sets, and a VB100 award is just about earned.

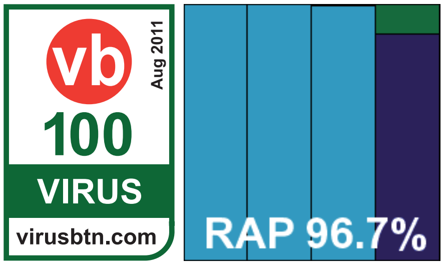
The history for this version of the formerly *CA*-owned product shows four passes, one fail and one no-entry in the last six tests; seven passes, three fails and two no-entries in the last two years. Other than the total incapacitation of the test systems caused by the failed updates, and the occasional corruption of logs when scans produce too many detections and drain too much memory, there were no other crashes or problems; nevertheless, thanks to a combination of slow scans of our infected sets, the logging problems and the failures to update, with related support calls and retests, the product hogged one of our test systems for more than ten days.

TrustPort Antivirus 2012

Program version 2012 (12.0.0.4778)

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

TrustPort's latest product was submitted as a 210MB package including updates, and installed in decent time with not too much interaction and no need for a reboot. The interface is a little unusual, but is easily deciphered and proved simple to operate, providing splendid configuration controls.



Speed tests were a little slow – as we expect from a multi-engine approach – but on-access overheads were not too bad, and resource use was OK too, with a fairly low impact on our set of jobs. Detection measures showed the usual stunning scores, with very little missed across all the sets. The WildList was covered easily, and with no problems in the clean sets *TrustPort* earns another VB100 award.

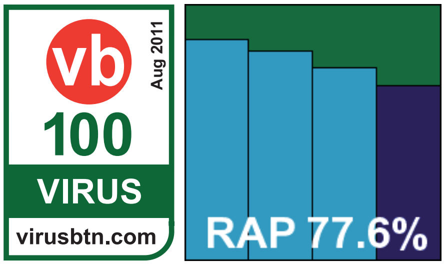
The vendor's history shows some good performances, with four passes from four attempts in the last six tests; nine from nine in the last two years. No problems emerged in testing, with everything running smoothly even under heavy fire, and all our work was done in under a day.

VirusBuster Professional

Version 7.1.70, Virus scan engine 5.3.0, Virus database 14.0.91

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.18%
Worms & bots	92.29%	**False positives**	0

Another fixture in our lists of participants, *VirusBuster* has only missed two tests in over a decade. The submission this month took the form of a 69MB installer and a 59MB update bundle, and the set-up process once again included the option to join a feedback scheme hidden away on the same screen as the EULA acceptance. Otherwise things were pretty standard, taking a little while to finish and needing a reboot to complete.



The interface hasn't changed its layout in many years, but has recently had a little refresh with a change of colour scheme and some other surface tweaks. The design itself remains a little awkward and clumsy in places but provides a decent degree of control.

Scanning speeds were not bad, and overheads reasonable too, with average use of resources and only a slightly higher than average hit on our set of tasks. Detection rates were pretty easy to gather with no stability problems, showing strong detection in the main sets and a reasonable showing in the RAP sets. The core certification sets were properly handled, and *VirusBuster* earns a VB100 award.

This is the vendor's sixth pass in the last six tests, the two-year view showing ten passes and two fails, with no tests skipped. The product behaved well throughout testing, completing in just a little over 24 hours.

CONCLUSIONS

A bit of a marathon this month, with testing taking its longest time ever to complete. Things were a little hampered by external problems including illness in the team and power issues which hit the lab. However, the main things slowing us down this month were the products themselves. While many, perhaps even most, behaved well and got through all the tests within the 24 hours of machine time allotted to each, several took considerably longer, with some needing more than a week and a couple taking almost three weeks. While we cannot disqualify a product for taking its time (as most of this is down to handling large sets of infected files – not something a product is likely to encounter in real-world use), we do hope developers will take us into account when designing their products and aim to make them at least slightly testable. It is of course not only we who are affected by this, but also vendor QA teams, who should also be performing heavy stress testing not unlike what we run as part of our comparatives.

Other issues have once again included logging problems, with some vendors apparently unable to decipher their own logs and several others unaware of whether or not their products retain all potentially useful information. The month has also seen a bumper crop of stability issues, with several products suffering blue screens and others crashing or freezing the system for long periods. This is something we may consider including as a possible reason to deny a product certification in future, and certainly all developers should be very worried if their products are causing such issues, even under heavy stress.

It's possible, of course, that much of this is down to the platform itself, which has proved an awkward one to work with. We're tempted to advise users in search of the right solution to protect their 64-bit *Vista* systems simply to give up and switch to a different platform. There was certainly agreement in the team that we should never revisit this platform, given the horrors of this month's test.

As well as all the bad, though, there were also some good things this month. Some products performed admirably, recording splendid scores and remaining steadfast despite all we could throw at them. One notable point is that not a single WildList sample went undetected by any of the products under test (although a few did seem to need a little gentle encouragement). As mentioned in the introduction, this month saw the public unveiling of an expansion to the current WildList system, known as the 'Extended WildList', which includes a wider range of malware types. We plan to include this as part of our certification requirements, effective immediately. This test is thus the last to include the WildList in its current form, and after an introductory test under the current conditions next time we plan to make some more radical changes to the way our tests operate. These will be detailed next month after consultation with our advisory board and other interested parties. As usual, all suggestions, requests and criticisms are welcomed.

Technical details

All products were tested on identical machines with *AMD Phenom II X2* 550 processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Microsoft Windows Vista,* 64-bit Business Edition, with Service Pack 2. For full testing methodology see http://www.virusbtn.com/vb100/about/methodology.xml.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Web Developer: Paul Hettler

Consulting Editors:
Nick FitzGerald, *Independent consultant, NZ*
Ian Whalley, *IBM Research, USA*
Richard Ford, *Florida Institute of Technology, US*

SUBSCRIPTION RATES

Subscription price for Virus Bulletin magazine (including comparative reviews) for 1 year (12 issues):

- Single user: $175
- Corporate (turnover < $10 million): $500
- Corporate (turnover < $100 million): $1,000
- Corporate (turnover > $100 million): $2,000
- *Bona fide* charities and educational institutions: $175
- Public libraries and government organizations: $500

Corporate rates include a licence for intranet publication.

Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):

- Comparative subscription: $100

See http://www.virusbtn.com/virusbulletin/subscriptions/ for subscription terms and conditions.

Editorial enquiries, subscription enquiries, orders and payments:

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park,
Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: http://www.virusbtn.com/

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.