virus

B U L L E T I N

Fighting malware and spam

VB100 COMPARATIVE REVIEW ON WINDOWS 7

INTRODUCTION

A glance through the list of entrants for this desktop test shows a fairly familiar line-up. However, between the commencement of the test and the completion of this report there have been a number of significant happenings in the industry, with companies being bought out and taken over, and products that have lengthy pedigrees ceasing to exist. Many people have long since predicted this sort of streamlining in the industry, but the general trend of late seems to have been towards diversification, with an ever wider range of products coming onto the market.

The resulting steady increase in the number of products participating in our comparatives continues to put a strain on our resources, and as of this test we have been forced to impose further limits on the number of products that can participate without charge. From now, each vendor will be entitled to one place in the test at no cost, and additional products will only be included for a fee (which will be waived for those companies that contribute to our costs through the VB100 logo licensing scheme).

This report also sees the introduction of a formalized version of the stability measures which have been mentioned in recent tests. They are now covered in more detail in a new table – eventually we hope to include a basic level of reliability as part of the requirements for VB100 certification. The new table, with results of the stability scoring system, is supplemented by some additional details such as the time taken to install products, and whether the technology involved is 'home-grown' or licensed from a third party. We hope to expand further on this data in future tests; for full details, particularly of the stability rating system, please refer to the appendix to this article.

PLATFORM, PRODUCTS AND TEST SETS

We return to *Windows 7* for this test with the release of its intended successor, *Windows 8*, just around the corner. Replacing the rather poorly received *Vista* just three years ago, *Windows 7* has done rather better and has just about managed to supplant *Windows XP* as the desktop of choice for most PC users. The platform has appeared in several tests already, and has generally generated very high levels of participation, although this month's numbers were not quite as high as we initially anticipated. This was in large part due to the absence of a cluster of products based on a single implementation of one of the more popular engines, but once again we saw a wide range of OEM solutions. Continuing a trend observed last time, *Bitdefender* took the reins as the most widely deployed engine, featuring in at least 13 of the 50 or so products taking part.

Preparing the test systems proved fairly straightforward, with test images used in the last *Windows 7* test unearthed and given a quick dusting down. The first and so far only service pack for *Windows 7* was released over two years ago, but no further updates were added to systems, unless specifically requested by product installers.

Test sets were deployed in the usual manner, with additions to the clean sets focusing on consumer software – several of the major download sites were scoured for the most popular and widely used items, and more items were added from magazine cover CDs and so on. So as not to neglect business users, the latest versions and updates of a number of common business productivity solutions were also added. The WildList sets were frozen on the test deadline of 24 June, which meant using the May list (released in early June). As usual, a number of revisions were made to the Extended WildList as items contained therein were challenged by participants, and further items were excluded

if our own processes deemed them to be unsuitable. The RAP sets and Response sets were compiled using the same formula, using a selection of samples gathered daily, and this month after final rounds of validation and analysis the RAP set ended up containing around 20,000 samples per week, while the Response sets measured around 2,500 samples per day on average. Testing commenced on 1 July, and with a few interruptions for staff holidays and further work on the expansion of our lab space, was finished (as far as the certification components were concerned) by the end of the month, the remaining performance measures and so on continuing into late August.

Agnitum Outpost Security Suite Pro

Main version: 7.5.2 (3939.603.1810)

Update versions: 20/6/2012, 10/7/2012, 18/7/2012, 23/7/2012

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			1

First up on this month's list is one of the companies at the heart of one of the big industry shake-ups in recent months. Having long enjoyed a close relationship with *VirusBuster*, including using the company's engine in the *Outpost* product, a month or so after submitting for this test *Agnitum* announced its plans to take over development of the *VirusBuster* engine, inheriting the source code and all intellectual property from the now defunct company. Thus the first of our tables detailing the source of third-party technology is rendered even more complicated than we had anticipated, as those products currently marked as containing the *VirusBuster* engine (including *Agnitum*'s own) will in future be marked as containing the *Agnitum* engine. For now, however, we will stick to the names of the products and technology as they were at the start of this test.
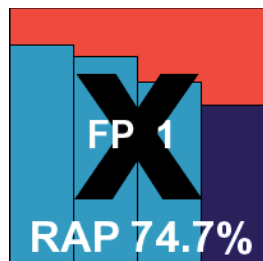
Outpost has been a regular in our tests for a while and has achieved a solid record, managing a streak of 12 consecutive passes. The product itself is well designed and usually pleasant to operate. The install package measured 115MB, including all required updates for the RAP tests, and took fewer than six clicks to install, although the process did take some time, much of it taken up with initialization processes for the firewall components. Updates were integrated into the overall process so it was hard to judge just how long the updating took, but the average

install time was a reasonable six minutes, with a reboot required to complete the process on each run.

On one occasion there was a major problem with the installation, when the machine failed to return to life properly after the reboot. After getting past the login prompt to the 'Welcome' screen, no further progress could be made, with the cursor responding to mouse actions but no other functionality available and even control-alt-delete had no effect. A hard reset didn't help, and with time pressing we opted to simply re-image the test system and try the install again. Fortunately, the problem did not recur, either then or during any subsequent installs, nevertheless with the issue appearing in normal use and causing major inconvenience it is classed as a major bug and counts heavily against *Agnitum*'s stability score.

Another issue was observed during the on-access testing against malware samples, when the machine seemed to enter some kind of lock-down mode, meaning that we couldn't check progress by opening log files in *Notepad* – error messages did not come from the product itself, but seemed to imply some problem with the operating system. Once the test job was complete, the system remained more or less unusable for around 15 minutes. This was a recurrent problem with all test runs, and although it only occurred during non-standard operations, when dealing with fairly large sets of malware samples, it adds further to the product's stability woes.

Otherwise all ran fairly smoothly though, the product interface being clear and well laid-out with a basic level of fine-tuning available, logging to easily readable plain text, with a size cap in place which is adjustable within limits. Scanning speeds were a little sluggish initially but rapid in the warm runs; overheads were likewise on the high side at first but much lighter once the files had initially been checked out. Resource use was on the high side, but our set of tasks ran through in decent time. Detection scores were a little mediocre, as usual, with a fairly steep drop through the weeks of the RAP sets, and we can only hope that the changes in the ownership and operation of the engine will bring some improvements.

The changeover period may have had some impact on the clean set coverage too, with a rare false positive observed: an item from *IBM* was flagged as the Psyme worm. This means that *Agnitum*'s run of success in the VB100 tests comes to an end just as the vendor prepares for a new era, leaving it on four passes and one fail in the last six tests, with no entries in our annual *Linux* tests; nine passes and one fail in the last two years. The serious issue with one of the installs, plus the lock-ups during the on-access tests, places the product just inside the 'buggy' category in our stability rating system.

AhnLab V3 Internet Security 8.0

Main version: 8.0.6.6 (Build 1197)

Update versions: 2012.06.20.01, 8.0.6.13 (Build 1239)/2012.07.10.00, 2012.07.16.05, 2012.07.21.00

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	99.95%
False positives			0

AhnLab has been rather inconsistent in its entries of late, with its last appearance having been in the previous *Windows 7* test in late 2011.

RAP 81.3%

The vendor returns in this test with much the same product as we remember from way back then. The current installer measures 208MB with latest updates included and runs through its business fairly rapidly, after a slightly worrying few moments of complete silence before it starts moving. Only a few clicks are required, with no need for a reboot at the end, and the entire process including online updates took under four minutes on average.

The interface is clean and clear, providing a reasonable degree of control, and it seemed responsive throughout testing, even under heavy pressure. Logs are displayed in a special viewer tool, which provides the option to save to text.

Scanning speeds were not too bad, and overheads perhaps just a little above average, with low use of resources and impact on our set of tasks noticeable, but not extravagant. Detection rates were not too bad, showing a relatively gentle decline through the RAP sets, and a similar slope in the Response sets from a decent starting point. With no problems in the core certification areas, a VB100 award is earned, giving *AhnLab* two passes and one fail from three attempts in the last six tests; four passes and three fails in the last two years. There were no bugs or stability issues noted, giving the product a 'solid' rating.
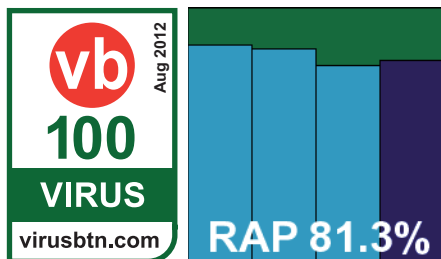
Auslogics Software Antivirus

Main version: 15.0.36

Update versions: 7.42872/7365118, 7.42915/7359988, 7.42961/7364417

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Auslogics has a single previous entry under its belt, again in the previous *Windows 7* test late last year. The product is a straight clone of *Bitdefender*'s current offering, with a few tweaks including the 'Dragon Wolf' that adorns *Bitdefender*'s install process having been changed to a simple 'Black Dragon' here. The set-up was run from a small downloader program, which fetched the latest build of the main installer. This initial download was very speedy, taking less than 15 seconds, and a standard set-up process then followed, including a zippy scan of vital areas and further downloading of components. The whole thing was done in under half a minute. Rather surprisingly, given the multiple download stages already witnessed, more updates were then required, but again these were very quick, taking only 20 seconds or so to fetch the 15MB of data requested.

On the initial installation, a quick check showed things were not quite right; no protection was in place and scanning appeared non-responsive. On digging further, we found a rather well-hidden message saying a reboot was needed to complete a stage, but even after several restarts we were unable to get things moving. An error message indicated that a key service was not running, but the *Windows Event Viewer* system claimed it was, and was blocked from trying to restart it. Re-running the installer brought an offer to repair the installation, which ran through and claimed to have made some fixes, but still the product refused to work. Having wasted enough time on our busy deadline day, we aborted the job hoping to be able to fix it later, but sadly had no luck, meaning that the RAP tests could not be performed; we would assume that, had things worked out properly, scores would closely match those of the *Bitdefender* solution.

When we came back a few weeks later and retried the install from scratch on a different system, everything went smoothly, with no repeat of these problems over multiple reinstalls – it looks like on our initial attempts we were hit by a very unlucky one-off bug. For the rest of testing everything went very nicely indeed, with blazing fast scan times especially in the warm runs, very light overheads until the settings were turned up, fairly low resource use and a light impact on our set of tasks. The design is clear and pleasant, with a good level of configuration available, and responsiveness was good throughout. Logging is kept in a fairly readable XML format, with no apparent option to export to more human-friendly plain text.

Detection rates were really quite excellent, with consistently high scores throughout the Response sets, no issues at all in the WildList sets and no false positives either. *Auslogics* thus comfortably earns its second VB100 award. That gives

Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Suspicious
Agnitum Outpost	100.00%	100.00%	100.00%	100.00%	1	11
AhnLab V3	100.00%	100.00%	100.00%	99.95%		
Auslogics Antivirus	100.00%	100.00%	100.00%	100.00%		
Avast Free Antivirus	100.00%	100.00%	100.00%	100.00%		
AVG Internet Security	100.00%	100.00%	100.00%	100.00%		
Avira Free Antivirus	100.00%	100.00%	100.00%	100.00%		
Avira Professional Security	100.00%	100.00%	100.00%	100.00%		
Bitdefender Antivirus Plus 2012	100.00%	100.00%	100.00%	100.00%		
BullGuard	100.00%	100.00%	100.00%	100.00%		
Central Command Vexira	100.00%	100.00%	100.00%	100.00%	2	5
CMC Internet Security	79.25%	69.05%	81.49%	68.03%	448	461
Commtouch Command Anti-Malware	100.00%	100.00%	100.00%	100.00%		
Comodo Antivirus	99.09%	98.40%	99.09%	98.40%		1
Coranti 2012	100.00%	100.00%	100.00%	100.00%		
Defenx Security Suite 2012	100.00%	100.00%	100.00%	100.00%	1	11
eEye Blink Professional	99.84%	100.00%	99.84%	100.00%		1
Emsisoft Anti-Malware	100.00%	99.93%	100.00%	99.93%		10
eScan Internet Security Suite	100.00%	100.00%	100.00%	100.00%		
ESET NOD32 Antivirus 5	100.00%	100.00%	100.00%	100.00%		
ESTsoft ALYac Enterprise	99.84%	99.85%	99.84%	99.80%		
Filseclab Twister Antivirus V7	95.47%	93.52%	95.47%	92.32%	114	6
Fortinet FortiClient	100.00%	100.00%	100.00%	100.00%		
Frisk F-PROT Antivirus	100.00%	100.00%	100.00%	98.85%		
F-Secure Client Security*	100.00%	100.00%	100.00%	95.92%		1
F-Secure Internet Security 2012	100.00%	100.00%	100.00%	100.00%		1
G Data AntiVirus 2013	100.00%	100.00%	100.00%	100.00%		

Full detection in place during two out of three runs.
Please refer to text for full product names.

Certification tests contd.	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Suspicious
GFI VIPRE Antivirus 2012*	100.00%	99.90%	100.00%	99.90%		
Hauri ViRobot Internet Security 2011	100.00%	100.00%	100.00%	100.00%		
Ikarus virus.utilities	100.00%	99.93%	100.00%	99.93%		5
Iolo System Shield	99.20%	98.40%	100.00%	100.00%		
K7 Total Security	100.00%	100.00%	100.00%	100.00%		
Kaspersky Endpoint Security	100.00%	100.00%	100.00%	100.00%		
Kaspersky Internet Security 2013	100.00%	100.00%	100.00%	100.00%		
Lavasoft Ad-Aware Free Antivirus +*	100.00%	99.90%	100.00%	99.90%		
McAfee VirusScan Enterprise	100.00%	100.00%	100.00%	100.00%		
Microsoft Security Essentials	100.00%	100.00%	100.00%	100.00%		
Norman Security Suite	100.00%	100.00%	100.00%	100.00%		
Optenet Security Suite	100.00%	99.90%	100.00%	99.90%		
Panda Cloud Antivirus PRO	100.00%	100.00%	100.00%	100.00%		
PC Tools Internet Security	100.00%	100.00%	100.00%	100.00%		
PC Tools Spyware Doctor	100.00%	100.00%	100.00%	100.00%		
Qihoo 360 Antivirus	100.00%	100.00%	100.00%	100.00%		8
Quick Heal Total Security 2012	100.00%	100.00%	100.00%	100.00%	1	
Roboscan Enterprise Solution	99.84%	99.85%	99.84%	99.80%		
Sophos Endpoint Security and Control	100.00%	100.00%	100.00%	100.00%		
Tencent PC Manager	100.00%	100.00%	100.00%	100.00%		
Total Defense Inc. Internet Security Suite	100.00%	100.00%	100.00%	100.00%		
Total Defense Inc. Total Defense r12	100.00%	100.00%	100.00%	100.00%		
TrustPort Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
VirusBuster Professional	100.00%	100.00%	100.00%	100.00%	2	5
ZeoBIT PCKeeper	100.00%	100.00%	100.00%	100.00%		

Full detection in place during two out of three runs.
Please refer to text for full product names.

the vendor two passes from two attempts, both in the last six tests. With the problems encountered in the first install not recurring, stability was rated as 'fair'.

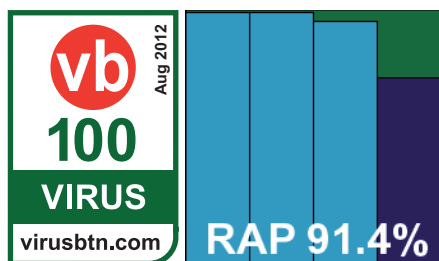## Avast Software avast! Free Antivirus

Main version: 7.0.1445

Update versions: 120620-1, 7.0.1458/120709-0, 120716-0, 120719-2

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The only blemish on *Avast*'s recent history is a fail in the last *Windows 7* comparative. The product routinely elicits

warm, affectionate smiles from the test team, with this month's submission promising more of the same. The install package measured 86MB and included all data required for the RAP tests. Later, online updates averaged around 45 seconds, including the additional time taken to update the full product on some occasions; at these times a reboot was needed to complete things, but usually this was not necessary. The install process itself is speedy and smooth, with the offer to install *Google*'s *Chrome* browser and some advertising for the company's upcoming *Android* offering the only reminders that this is a free solution.

The interface itself remains one of the most satisfyingly clear and usable out there, packaging an impressive range of functions into a slick and at times quite beautiful GUI. Configuration options are provided in unimpeachable depth and for the most part maintain splendid levels of clarity and simplicity, although a few spots do seem to rely on existing knowledge of the product's few quirky concepts. Logging is clear and simple to use, although it seems to be switched off by default in most areas. In the past we have seen some wobbliness in the sandboxing components, but this was not evident this month – hopefully due to fixes rather than simply good luck.

Scanning speeds were pretty decent and our overhead measures fairly light, although the product only does limited on-read scanning by default; with the settings turned up things did slow down a little, but not terribly. Resource use was around average, with impact on our set of tasks perhaps slightly higher than some.

Detection rates were very decent, with some superb scores in the reactive parts of the RAP test but a fairly sharp drop into the proactive week. The Response sets also showed high numbers in the earlier days and a bit of a downturn in the last day or two. The core sets were properly dealt with though, and *Avast* earns another VB100 award fairly easily; that gives the vendor five passes and just one fail in the last six tests; 11 passes out of 12 entries in the last two years. With no issues to report, stability was rated a firm 'solid'.

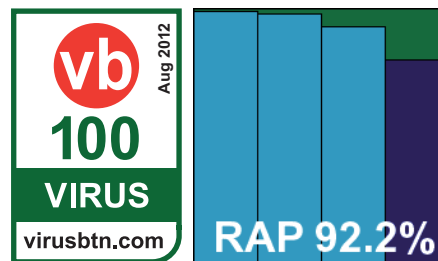## AVG Internet Security Business Edition

Main version: 2012.0.2180

Update versions: 2437/5079, 2437/5121, 2012.0.2195/2437/5135, 2012.0.2197/2437/5142

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

In contrast to its compatriot *Avast*, *AVG* tends to submit its paid-for business suites rather than its wildly popular free offerings. This month is

no different, with a fairly large 148MB installer provided, including required updates for the RAP tests. Set-up was very speedy and simple, with an 'Express' install option meaning that only a couple of clicks were needed. Updates were also very rapid, the whole process taking less than two minutes to complete with no reboots required.

The interface is cleaner and leaner these days, providing a decent if not quite exhaustive set of controls, and logging was fairly clear and usable too. Responsiveness was generally good, but on one of the installs things seemed to get a little snarled up – scanning refused to start, with no error message or explanation for its silence, and a reboot was needed to get things moving again. After that all seemed fine though, and there was no sign that the issue had affected protection.

Speeds were pretty good, with serious improvements in the warm runs. Overheads were extremely light, although resource use was a little high and our set of tasks took a fair time to get through. Detection was good though, with pretty decent scores across the board, and with no issues in the core sets a VB100 award is duly earned. *AVG* now has five passes and one fail in the last six tests, ten passes and two

fails in the last two years. With a single, non-reproducible issue noted, the product earns a 'stable' rating.
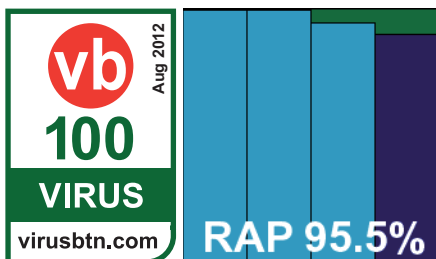
Avira Free Antivirus

Main version: 12.0.0.1125
Update versions: 7.11.33.62, 7.11.35.136, 7.11.36.94, 7.11.36.252

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another seriously popular free product, *Avira*'s basic offering was provided as a mid-range 96MB installer, with an additional 68MB of updates for offline use. Installation was via another 'Express' system involving little more than a single click, plus acceptance of a EULA, and completed very rapidly. Updates were mostly very speedy, generally taking less than 30 seconds, but on one of the runs for some reason this was dragged out to over 10 minutes. This brought the total install average to just over four minutes.

The interface is a little crisper and friendlier these days, and provides a good level of control, although this is somewhat hampered in some areas such as by the absence of an option to scan a specific area from the main GUI (a context-menu scan option is of course provided). Logging is in plain text and laid out in a human-friendly format. Things seemed to work OK most of the time, but on one occasion the scanner component crashed out with a rather ungrammatical error message, claiming that 'the exception unknown software exception occurred'. Restarting the scan was not a problem, and we didn't manage to get this behaviour to recur. As it happened during an on-demand scan of a large malware set, it did not dent the product's stability rating too heavily.

Scanning speeds were very good, as ever, and lag times fairly light, with RAM use low and CPU use a little below average, as was impact on our set of tasks. Detection rates were very solid indeed, with high scores everywhere, and the core sets caused no problems either, earning *Avira* a VB100 award for its free solution. Participating only in desktop comparatives, it now has three passes from three attempts in the last six tests; six from six in the last two years. With just a single minor crash noted, the product is rated as 'stable'.
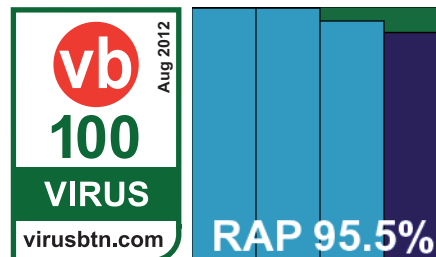
Avira Professional Security

Main version: 12.0.0.1466
Update versions: 7.11.33.62, 7.11.35.136, 7.11.36.94, 7.11.36.252

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Very similar in most respects to the free edition, *Avira*'s Pro version has a few little extras which are usually most noticeable to us in the additional configuration available in some areas. The set-up was similarly simple and speedy, with no issues encountered zipping through the updates this time and an average install time of less than two minutes.

With a few additional areas that are not found in the free edition, such as a more complete scanner interface, the controls are highly rated for thoroughness, and logging is clear, lucid and reliable. Once again we noted an issue in the RAP tests, with the scanner crashing out unexpectedly, but again the task was re-run with no repeat of the problem.

Scanning speeds were good and overheads not bad, with low memory consumption, reasonable use of CPU cycles and our set of tasks completing in good time. Detection scores were excellent, with the drop-off in the proactive week of the RAP sets especially slight, and with no issues in the WildList or clean sets a second VB100 is easily earned by *Avira* this month. That keeps the Pro offering's flawless run of success going: 12 passes in the last 12 tests. Stability was hit by a single scanner crash, which again occurred only while scanning a large set of samples; the rating is thus 'stable'.
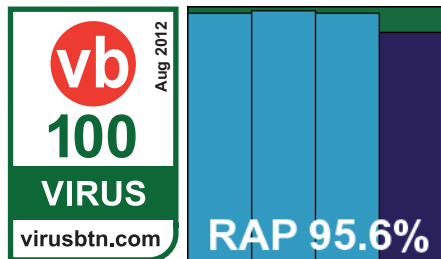
Bitdefender Antivirus Plus 2012

Main version: 15.0.31.1283
Update versions: 7.42671/7313010, 7.42867/7363718, 7.42915/7359988, 7.42961/7364417

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Having become the most popular engine for inclusion in other products, *Bitdefender*'s solution has already appeared this month

with only the most minor of alterations. A wider range of implementations is yet to come, and things already look promising. The initial installer provided here included all updates required for the RAP test, weighing in at a fairly hefty 212MB; on running it, it immediately offered to download a fresh version – when this was required, it rarely took more than 30 seconds, presumably only fetching a fairly recent version of the main installer, as further updates would still be required later on. The main set-up involves only a couple of clicks and completes in good time, with definition updates adding no more than half a minute or so in most cases.

The recently refreshed interface is a little dark and brooding, but fairly attractive and easy to navigate. Options are provided in great depth, with good clarity; logs are stored in an XML format which is fairly simple to read with the naked eye, and seem quite reliable since some issues with excessively large logs were resolved several tests ago.

Scanning speeds were reasonable from the off, with huge improvements in the warm runs. On a couple of occasions these scan jobs (of clean files only) did seem to freeze up after a few seconds and had to be restarted, but this was not a reliably reproducible problem. File access times were perhaps a little sluggish, especially with settings turned up to the maximum thoroughness, but not too intrusive. Resource use was barely noticeable, and our set of tasks didn't take too much longer than normal to complete.

Detection rates were extremely impressive, with excellent figures in both the RAP and Response sets. The core sets proved no problem either, and *Bitdefender* easily earns a VB100 award; it too joins the elite club of vendors celebrating 12 successive VB100 passes. With only a single very minor issue noted, a 'stable' rating is earned.
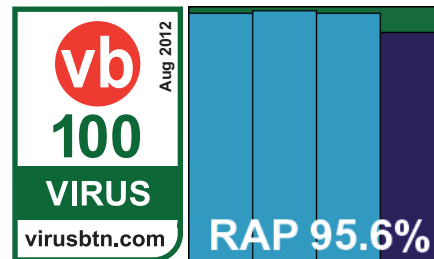
BullGuard

Main version: 12.0.224

Update versions: 12.0.0.29/12.0.0.27/12.0.0.58/12.0.0.50

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives			0

As one of our longest-serving *Bitdefender*-based products, we expected good things from *BullGuard* too. The initial installer was mid-sized at

147MB and installed very speedily with only a few clicks, reboots were required on some updates. Updating took between ten seconds and a couple of minutes, much of which was 'implementing' rather than downloading in the longer runs.

The interface is a little quirky but reasonably simple to operate, providing just a little more than the bare minimum set of controls. Logs can be saved in a '.bglog' XML format, which is clearly displayed in the product's own viewer tool but less friendly for separate processing.

Speeds were splendid, with more great improvement in the warm runs. Overheads were fairly light, RAM use was low but CPU use rather high, while our set of tasks got through in average time. Detection was again really quite excellent, with very little overlooked in any of the sets. The core sets were perfectly handled and *BullGuard* also earns a VB100 award, giving it five passes from five entries in the last six tests; nine from nine in the last two years. No issues were noted, earning it a 'solid' rating.

### Central Command Vexira Antivirus Professional

Main version: 7.4.68

Update versions: 5.5.1.3/15.0.62.1, 5.5.2.10/15.0.91.0, 5.5.2.11/15.0.102.0, 5.5.2.13/15.0.111.0

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	100.00%
False positives			2

Another product based on the engine formerly known as *VirusBuster*, *Central Command*'s *Vexira* is a regular in our tests and usually causes few major problems. The set-up process follows the usual lines, with the option to join a feedback scheme rather deviously hidden on the EULA acceptance page;
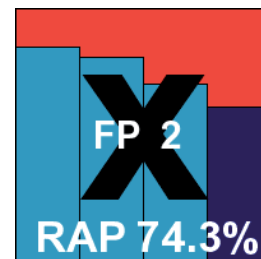
it completed in around two minutes on average. Updating

was less speedy – on several occasions initial attempts failed with little or no information, while trying to re-run the process seemed to do nothing. Leaving it alone to do its thing seemed the best if not *only* way to achieve a proper update, and getting this to occur took anywhere from five to 90 minutes, for no discernible reason – our average install time is thus a rather rough estimate of the average user's chances.

The interface is a little clunky and old-fashioned, but reasonably usable with a little practice, and provides a decent level of configuration. Logging is capped for size but adjustable within limits, and produces reliable and pleasantly readable text logs. Scanning was not the fastest, and overheads were a little heavy in some areas, with low resource use and a fairly low impact on our set of tasks.

Detection rates were a little mediocre in most areas, but the WildList was handled well. However, with all looking good, a couple of false positives turned up in the clean sets, including the *IBM* item noted earlier, thus denying *Vexira* a VB100 award on this occasion. The product now has four passes and two fails from the last six tests; eight passes and two fails in the last two years. With the updating problems the only issue noted, but a fairly serious one, stability is rated only 'fair'.

## CMC Internet Security

Main version: 1635
Update versions: 1637

ItW Std	79.25%	**ItW Std (o/a)**	81.49%
ItW Extd	96.05%	**ItW Extd (o/a)**	68.03%
False positives			448

A newcomer of sorts, *CMC* makes its first appearance in a set of results here, but the vendor has submitted products several times before. The fact that previous attempts to coax the product through the testing process have invariably failed did not bode well. With problems a little more manageable this month, we bravely soldiered through to gather a reasonably complete set of figures. The installer provided measured 67MB, and initial set-up seemed fairly smooth, with the standard set of steps to click through, completing in around a minute with no need to reboot.

FP 448
RAP 61.6%

The interface is fairly clear and simple to navigate, providing a basic set of controls, and while not as slick and glossy as some, it looks businesslike and professional.
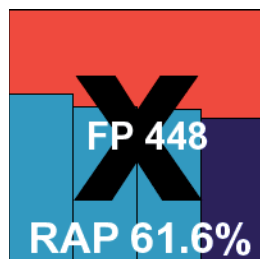
Problems hit us immediately though, with updates routinely seizing up. The update process fetches a fair number of distinct items, and on some occasions the number remaining would go down with each attempt, hinting that at least some progress was being made, while on others restarting the job set things back to the very beginning. On occasion a message would warn that the 'CMCcore' had stopped working, and nothing could be done to get it back online; in these cases (around one in three installs) we had no option but to wipe the machine and start again from scratch.

We generally managed to get a functioning and apparently at least mostly updated product to work with though, and plodded on through the tests. Speed tests were reasonably problem-free, with some fairly sluggish times, especially over the set of executables and other binaries; it was difficult to tell if archives were being properly examined, as there seemed to be no detection of the EICAR test file, rendering our archive depth test useless. Although convention suggests that failing to spot this file means the product is not set up properly, we did manage to get some detection of other items, both on access and on demand, so hopefully we had done nothing too wrong. On-access figures suggest some smart caching of previously scanned files, taking overheads from a little above average to quite decent in the warm runs, while resource use shows fairly average figures for RAM and CPU. Impact on our set of tasks was very high indeed, with a long time taken to get through the set of jobs.

On-demand tests were rather trying, with scans frequently crashing out with little data to report, but by carefully splitting the test sets into small chunks and running many small scans, we managed to get as close to a full set of figures as could be hoped for in the time available. Looking through the logs, it was clear that a large number of items were marked as variations of 'Heur:UNPACKED' followed by a common packer type such as UPX. While we would normally class such alerts as suspicious only (rather than full detections), given the large numbers of them evident in the WildList sets they were initially counted as full detections, but even with this concession, both the standard and Extended WildLists were not very well covered, with large numbers of misses in each. Ignoring the packed alerts reduced the figures by around a further 10%, but to be generous we allowed the alerts to stand.

We were also generous in the other direction in the clean sets, separating the alerts and counting the packer warnings as suspicious only, but even so false positives were rife. Even in our speed sets, specially compiled to minimize the chances of false alarms, a number of items were flagged, and when scanning the system's C: partition we even noted that components of the product itself were flagged as packed with UPX and thus potentially

Product information	Install time (mins)	Reboot required	Third-party engine technology	Stability score	Stability rating
Agnitum Outpost	5	Y	VirusBuster*	17.5	Buggy
AhnLab V3	4	N	-	0	Solid
Auslogics Antivirus	3	S	Bitdefender	5	Fair
Avast Free Antivirus	3	S	-	0	Solid
AVG Internet Security	2	N	-	1	Stable
Avira Free Antivirus	4	N	-	1	Stable
Avira Professional Security	1.5	N	-	1	Stable
Bitdefender Antivirus Plus 2012	2.5	S	-	1	Stable
BullGuard	2.5	S	Bitdefender	0	Solid
Central Command Vexira	23	Y	VirusBuster*	5	Fair
CMC Internet Security	47	N	-	64	Flaky
Commtouch Command Anti-Malware	3	N	Frisk†	1	Stable
Comodo Antivirus	7	Y	-	0	Solid
Coranti 2012	4.5	N	Lavasoft/GFI, Frisk, Bitdefender	1	Stable
Defenx Security Suite 2012	5	Y	VirusBuster*	7.5	Fair
eEye Blink Professional	13	N	Norman	0	Solid
Emsisoft Anti-Malware	3.5	N	Ikarus‡	15	Buggy
eScan Internet Security Suite	8	YY	Bitdefender	20	Buggy
ESET NOD32 Antivirus 5	4.5	N	-	1	Stable
ESTsoft ALYac Enterprise	8	N	Bitdefender	1	Stable
Filseclab Twister Antivirus V7	4	Y	-	0	Solid
Fortinet FortiClient	2.5	N	-	1	Stable
Frisk F-PROT Antivirus	3	Y	-	2.5	Stable
F-Secure Client Security	22	N	Bitdefender	16	Buggy
F-Secure Internet Security 2012	7	N	Bitdefender	2	Stable
G Data AntiVirus 2013	3	Y	Avast, Bitdefender	0	Solid

VirusBuster engine now owned by Agnitum

† Frisk now owned by Commtouch

‡ Future versions will include Bitdefender engine

S - Reboot required after some updates

O - Reboot optional, only required for some components

YY - More than one reboot required on some installs

0 = Solid

0.1 - 4.9 = Stable

5 - 14.9 = Fair

15 - 29.9 = Buggy

30+ = Flaky

Please refer to text for full product names.

Product information contd.	Install time (mins)	Reboot required	Third-party engine technology	Stability score	Stability rating
GFI VIPRE Antivirus 2012	4	N	-	5	Stable
Hauri ViRobot Internet Security 2011	5	N	Bitdefender	19	Buggy
Ikarus virus.utilities	4	N	-	6	Fair
Iolo System Shield	2	Y	Frisk[†]	0	Solid
K7 Total Security	1.5	N	-	0	Solid
Kaspersky Endpoint Security	14	S	-	1	Stable
Kaspersky Internet Security 2013	5	N	-	3	Stable
Lavasoft Ad-Aware Free Antivirus +	3	Y	GFI	39.5	Flaky
McAfee VirusScan Enterprise	4	O	-	0	Solid
Microsoft Security Essentials	2	N	-	0	Solid
Norman Security Suite	8	Y	-	0.5	Stable
Optenet Security Suite	43	Y	Kaspersky	4	Stable
Panda Cloud Antivirus PRO	0.5	N	-	2	Stable
PC Tools Internet Security	5	N	-	12	Fair
PC Tools Spyware Doctor	5	N	-	4	Stable
Qihoo 360 Antivirus	3	N	Bitdefender	1.5	Stable
Quick Heal Total Security 2012	2	N	-	0	Solid
Roboscan Enterprise Solution	11	N	Bitdefender	1	Stable
Sophos Endpoint Security and Control	4	N	-	0	Solid
Tencent PC Manager	2	N	Avira	0	Solid
Total Defense Inc. Internet Security Suite	3	Y	-	7	Fair
Total Defense Inc. Total Defense r12	4	YY	-	2	Stable
TrustPort Antivirus 2013	3.5	N	Bitdefender	0	Solid
VirusBuster Professional	18	Y	-	5	Fair
ZeoBIT PCKeeper	1	N	Avira	3	Stable

[*] *VirusBuster engine now owned by Agnitum*

[†] *Frisk now owned by Commtouch*

[‡] *Future versions will include Bitdefender engine*

S - Reboot required after some updates

O - Reboot optional, only required for some components

YY - More than one reboot required on some installs

0 = Solid

0.1 - 4.9 = Stable

5 - 14.9 = Fair

15 - 29.9 = Buggy

30+ = Flaky

Please refer to text for full product names.

dangerous. It would seem fairly basic logic that if one is going to warn about packers as a suspicious thing for a legitimate developer to be using, one should avoid using such packers oneself.

So, there is no VB100 award for *CMC* on its first full appearance in our tests, and it looks like quite some work is required for it to reach the required standard. With problems rife, the product stands very firmly in the 'flaky' category.
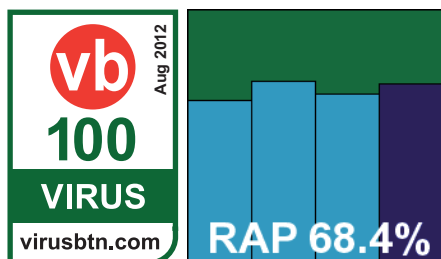
Commtouch Command Anti-Malware

Main version: 5.1.16

Update versions: 5.3.14/201206201558, 201207111323, 201207171158, 201207231225

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Our new table shows *Commtouch* as incorporating the *Frisk* engine, but in another acquisition that took place during the testing period it seems the roles may have to be reversed. *Frisk* now forms part of *Commtouch* and so perhaps in future *Frisk* will be described as using the *Commtouch* engine in its products (which seem set to continue as a separate line). *Commtouch* itself has had a rather rocky time in our tests of late.

The product was provided as a very compact 12.6MB installer, with an update package of 28MB for use in the RAP tests. Installing is fairly straightforward, involving only a couple of clicks and a few minutes' wait, while updates were very rapid indeed, taking no more than 20 seconds. No reboots were required.

The product interface is fairly rudimentary, but provides a basic set of controls which were mostly fairly responsive. Logs can be exported to readable plain text, which took quite some time when large amounts of data were being handled but never failed to complete. On one occasion the interface froze up on the completion of a scan, but forcing it to close cleared things up without difficulties.

Scanning speeds were not bad but lag times were very high, and while RAM use was low, CPU use was very heavy

indeed and our set of activities took an extremely long time to get through. Detection rates were not very good at all in the RAP sets but much better in the Response sets, implying some effective use of cloud-based technology that is not available when offline.

The WildList and clean sets were handled well, and *Commtouch* can celebrate a VB100 award this month, putting it on two passes and three fails in the last six tests; five passes and five fails in the last two years, with false positives the usual cause of trouble. With only a single, very minor issue noted, while scanning large infected sets, a 'stable' rating is earned.

Comodo Antivirus

Main version: 5.9.221665.2197

Update versions: 12889, 12973, 13031

ItW Std	99.09%	**ItW Std (o/a)**	99.09%
ItW Extd	98.40%	**ItW Extd (o/a)**	98.40%
False positives			0

Comodo has been quiet for a while as far as our test bench is concerned, the vendor's last entry having been late last year. Although the company has managed a single pass with its suite product, the standalone AV solution has been unlucky not to have made the grade yet. With the new fee structure in place, *Comodo* chose only to enter a single product (the standalone version), but the suite solution runs from the same installer, and provides the same malware detection alongside additional functions such as firewalling.

Set-up from the 84MB executable provided runs through a few steps, including the option to set the system's DNS to use *Comodo*'s servers. Online updating pulled down around 120MB of additional data on average, and took quite a while to do so – around five minutes in most runs. A reboot was required after updating, and in some cases this was rather hard to spot – it was mentioned in passing in the product's interface but not pointed out more forcefully. The GUI itself is colourful and attractive, appearing to provide a wealth of functions and options without becoming cluttered, and it seemed responsive throughout testing. Logging can be exported to a clear plain text format.

The company was unable to provide the product with updates from the deadline date, so for the RAP test an update was required on the day itself. Unfortunately, due to an administrative error, the image taken at this time was destroyed, so sadly no RAP figures can be provided. Other tests ran smoothly though, with fairly decent scanning speeds and rather heavy overheads; resource use was light however, and our set of activities didn't take too long.

Detection rates took rather a long time to gather in the case of the on-access measures, each run lasting more than an hour where most other products got through the same job in less than a minute. On-demand scanning was much more speedy. Response scores were not far behind the leaders, but in the WildList sets a few items were not detected, thus denying *Comodo* a VB100 award this time around. This product has no passes so far, from three entries in the last six tests and five entries in the last two years. There were no issues with stability, earning the product a 'solid' rating.
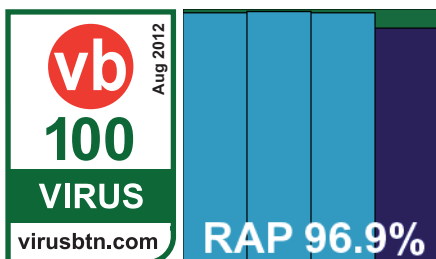
Coranti 2012

Main version: 1.005.00006

Update versions: 22318, 22537, 22593, 22649

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another vendor that requires us to install and update the product on the deadline day for the RAP tests, and another that would normally have

submitted a pair of products, until the recent change in the number of products that can be submitted free of charge. *Coranti* opted to submit its mainline product rather than the 'Cora' offshoot, and provided it as a svelte 53MB installer. This ran through after just a few clicks in less than half a minute, updates taking a little longer as over 230MB of data had to be fetched to feed the multiple engines included. This generally took no more than a few minutes though, and things were soon up and running.

The interface is fairly simple – wordy, but not too hard to find one's way around; configuration is decent but not exhaustive. One extremely minor issue was noted, in that while the interface insists the default setting for archive scanning is two levels of nesting, this was clearly not the case, with some types only opened to a single layer and others to at least ten. Scanning was initially rather sluggish, but picked up a lot in the warm runs, while on-access lag times were not too heavy. A lot of memory was used, but CPU usage was on the low side and our set of tasks was completed in good order.

As expected from the multi-engine approach, detection rates were very good indeed, with only the last day of the

Response sets dropping below 99% (and even then only very slightly), and the RAP sets covered excellently, scoring over 90% even in the proactive week. The WildList caused no problems at all, and with no false alarms either *Coranti* picks up another VB100 award with some ease. The vendor now stands at three passes from three entries in the last six tests for this product; six passes from eight entries in the last two years. With a single very minor defect noted, a 'stable' rating is earned.

Defenx Security Suite 2012

Main version: 3735.603.1669

Update versions: 20/06/2012 (9119179), 10/07/2012 (9225417), 18/07/2012 (9237307), 23/07/2012 (9246767)

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			1

Incorporating what should now be referred to as exclusively *Agnitum* technology, *Defenx* has become a fixture on our test bench in the last few years, and has built up an impressive record of success. The current version came as a 111MB installer, which ran through the usual stages, including the hidden option to join a feedback programme tucked away on the EULA page. A number of

tasks are then performed, including getting the firewall components settled in before running an initial update. This generally took around three minutes, bringing the total install time to just under five minutes in all. The product interface is similar to that of *Agnitum*'s own, with a fairly clear and simple layout, configuration for the anti-malware component more than basic but less than thorough. Logging is capped by default but this can be extended, and information is stored in a clear, readable text format.
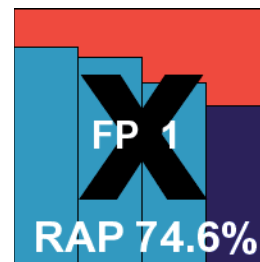
The speed tests passed without incident, showing some slowish times initially, but much better in the warm runs, while on-access overheads were very low indeed. RAM use was fairly low, CPU use decidedly high, and our set of activities ran through rather slowly too. The on-access measures over infected sets once again brought the machine to something of a standstill, with the opening of text files in *Notepad* and many other basic functions blocked and everything very slow for quite some time afterwards, as the deluge of detections was processed.

Detection rates, when finally worked out, were not terrible, but far from impressive, and although the WildList sets were

| 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	187.83	2.21	1820.96	2.21	13.18	997.14	13.18	15.54	2104.96	34.32	21.91	1144.05	21.91
AhnLab V3	26.49	5.62	8.01	5.62	31.89	33.53	31.89	24.44	54.75	53.97	47.66	53.46	47.66
Auslogics Antivirus	170.25	5.22	1820.96	5.22	49.72	6314.88	49.72	46.88	6314.88	103.52	73.33	3813.11	73.33
Avast Free Antivirus	120.51	5.28	5.67	5.28	21.41	21.31	21.41	23.44	52.19	51.76	54.47	53.46	54.47
AVG Internet Security	318.79	10.41	1366.06	10.41	35.48	1262.98	35.48	68.09	1578.72	150.35	62.51	1271.04	62.51
Avira Free Antivirus	193.74	5.99	6.00	5.99	27.94	29.10	27.94	55.00	126.30	121.44	63.55	71.95	63.55
Avira Pro Security	213.37	5.95	5.98	5.95	48.58	50.79	48.58	28.89	65.78	63.79	59.58	68.50	59.58
Bitdefender AV Plus	185.22	4.98	15.01	4.98	26.20	6314.88	26.20	24.03	6314.88	53.07	14.50	3813.11	14.50
BullGuard	67.64	5.32	1820.96	5.32	44.47	574.08	44.47	55.00	653.31	121.44	73.33	423.68	73.33
Central Command Vexira	211.68	2.80	2.75	2.80	15.36	15.47	15.36	24.87	55.23	54.91	31.78	31.95	31.78
CMC Internet Security	50.17	7.95	7.92	NA	6.60	6.59	NA	47.66	114.82	NA	29.11	28.74	NA
Commtouch Command	149.28	6.85	6.92	6.85	18.57	18.89	18.57	20.00	45.00	44.16	27.83	28.11	27.83
Comodo Antivirus	129.06	2.81	2.70	2.81	24.48	24.54	24.48	24.87	55.23	54.91	29.33	29.64	29.33
Coranti 2012	156.28	3.54	496.71	3.52	10.20	161.92	10.22	14.44	83.46	32.38	35.97	168.23	35.97
Defenx Security Suite	135.62	2.23	10.67	2.23	15.40	131.56	15.40	26.00	233.88	57.41	28.89	197.23	28.89
eEye Blink Professional	47.23	0.81	0.65	NA	8.67	7.20	8.67	26.73	58.83	59.02	38.91	39.18	38.91
Emsisoft Anti-Malware	245.45	14.57	14.61	14.57	32.38	52.19	32.38	29.79	74.59	65.78	52.23	61.17	52.23
eScan I.S.S.	155.37	151.75	182.10	NA	57.93	60.53	57.93	43.33	101.85	95.68	79.44	84.11	79.44
ESET NOD32	620.28	10.47	1820.96	10.47	26.42	574.08	26.42	49.31	2368.67	108.88	105.92	336.46	105.92
ESTsoft ALYac	150.12	4.63	4.82	4.63	50.52	126.30	50.52	31.78	357.46	70.17	65.74	190.66	65.74
Filseclab Twister AV V7	73.41	1.34	1.44	1.34	16.40	16.42	16.40	12.54	27.62	27.70	23.39	22.08	23.39
Fortinet FortiClient	81.48	9.44	11.57	9.44	15.48	17.91	15.48	24.44	63.57	53.97	26.67	30.10	26.67
Frisk F-PROT Antivirus	167.40	10.35	10.23	10.35	17.64	17.74	17.64	38.65	88.94	85.34	90.79	93.00	90.79
F-Secure Client Security	336.20	8.39	1820.96	5.69	38.74	1457.39	37.15	105.92	3157.44	65.10	190.66	2288.78	23.25
F-Secure I.S. 2012	769.38	8.93	1820.96	5.57	41.55	1578.72	41.01	98.61	6314.88	51.76	476.64	3813.11	24.44
G Data AntiVirus 2013	297.46	4.27	1820.96	4.27	23.30	1353.38	23.30	21.83	2104.96	48.21	39.31	3813.11	39.31

[*] *System drive size measured before product installation.*

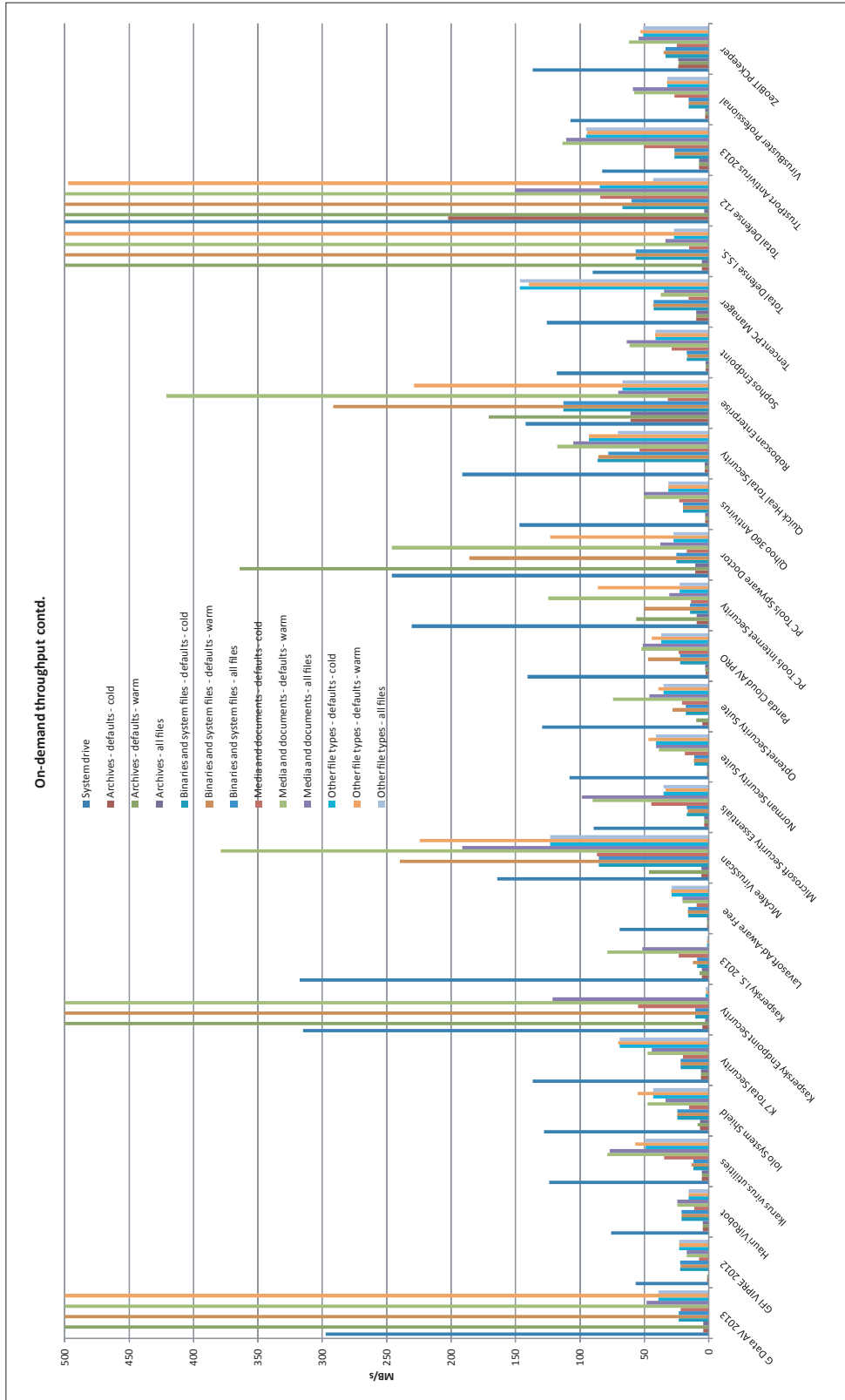*Please refer to text for full product names.*

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
GFI VIPRE Antivirus	56.91	1.32	1.32	NA	22.39	21.93	22.39	7.75	17.01	17.11	22.97	23.16	22.97
Hauri ViRobot I.S.	75.84	4.73	4.71	4.73	21.19	21.10	21.19	11.13	24.51	24.57	15.56	15.52	15.56
Ikarus virus.utilities	123.86	5.34	5.35	5.34	11.91	13.35	11.91	34.88	78.94	77.01	48.89	57.20	48.89
Iolo System Shield	127.82	6.82	8.56	6.82	24.38	24.35	24.38	15.21	47.48	33.59	43.33	55.26	43.33
K7 Total Security	136.78	6.09	6.12	6.09	21.78	21.88	21.78	20.00	47.72	44.16	69.33	70.18	69.33
Kaspersky E.S.	315.02	4.87	1820.96	2.97	10.56	1578.72	10.56	55.00	1894.65	121.44	2.57	2.12	2.57
Kaspersky I.S.	317.52	5.40	7.20	5.40	8.93	12.47	8.93	23.44	78.61	51.76	1.39	1.40	1.39
Lavasoft Ad-Aware	69.16	1.37	1.38	1.37	15.95	16.23	15.95	9.25	20.26	20.44	28.89	29.18	28.89
McAfee VirusScan	164.30	5.74	46.30	5.74	85.34	239.81	85.34	86.66	378.91	191.36	123.00	224.30	123.00
Microsoft S.E.	89.40	3.66	3.41	3.66	17.21	16.55	17.21	44.68	90.21	98.67	34.98	33.65	34.98
Norman Security Suite	107.98	1.30	1.31	1.30	11.26	11.62	11.26	18.57	38.82	41.01	41.00	46.69	41.00
Optenet Security Suite	129.47	5.10	9.70	NA	17.69	28.02	17.69	20.87	74.29	46.09	34.98	39.18	34.98
Panda Cloud AV PRO	140.87	2.48	2.88	2.89	22.39	47.36	22.39	23.25	52.48	51.34	37.02	44.34	37.02
PC Tools I.S.	230.59	9.24	56.32	9.24	14.38	50.25	14.38	13.95	124.64	30.80	22.56	86.01	22.56
PC Tools S.D	246.20	10.65	364.19	10.65	25.26	185.73	25.26	17.12	246.04	37.81	27.24	123.00	27.24
Qihoo 360 Antivirus	147.09	2.78	2.79	2.78	19.98	20.13	19.98	22.88	50.65	50.52	31.26	31.43	31.26
Quick Heal TS 2012	191.42	3.33	3.31	3.32	86.51	85.72	77.96	53.96	117.67	105.25	93.00	93.00	70.61
Roboscan Enterprise	142.12	60.70	170.73	60.70	112.77	291.47	112.77	31.78	420.99	70.17	66.90	228.80	66.90
Sophos E.S.C.	118.19	2.47	2.47	2.47	17.16	16.90	17.16	28.89	61.51	63.79	41.45	41.75	41.45
Tencent PC Manager	125.81	9.84	9.88	9.84	42.67	43.06	42.67	15.80	37.44	34.89	146.66	139.51	146.66
Total Defense I.S.S.	90.21	5.34	780.52	5.34	56.89	1114.52	56.89	15.21	1262.98	33.59	27.04	715.00	27.04
Total Defense T.D. r12	909.27	202.33	910.48	3.44	67.18	789.36	60.14	84.11	947.33	150.35	84.74	497.41	43.33
TrustPort Antivirus	82.66	7.62	7.57	7.62	26.76	26.72	26.76	50.17	113.44	110.79	95.33	94.54	95.33
VirusBuster Professional	107.55	2.83	2.81	2.83	15.63	15.72	15.63	26.73	57.93	59.02	32.31	32.50	32.31
ZeoBIT PCKeeper	136.78	23.65	23.25	23.65	33.59	34.95	33.59	24.65	61.91	54.44	50.84	52.96	50.84

System drive size measured before product installation.

Please refer to text for full product names.

On-demand throughput

Please refer to text for full product names.

On-demand throughput contd.
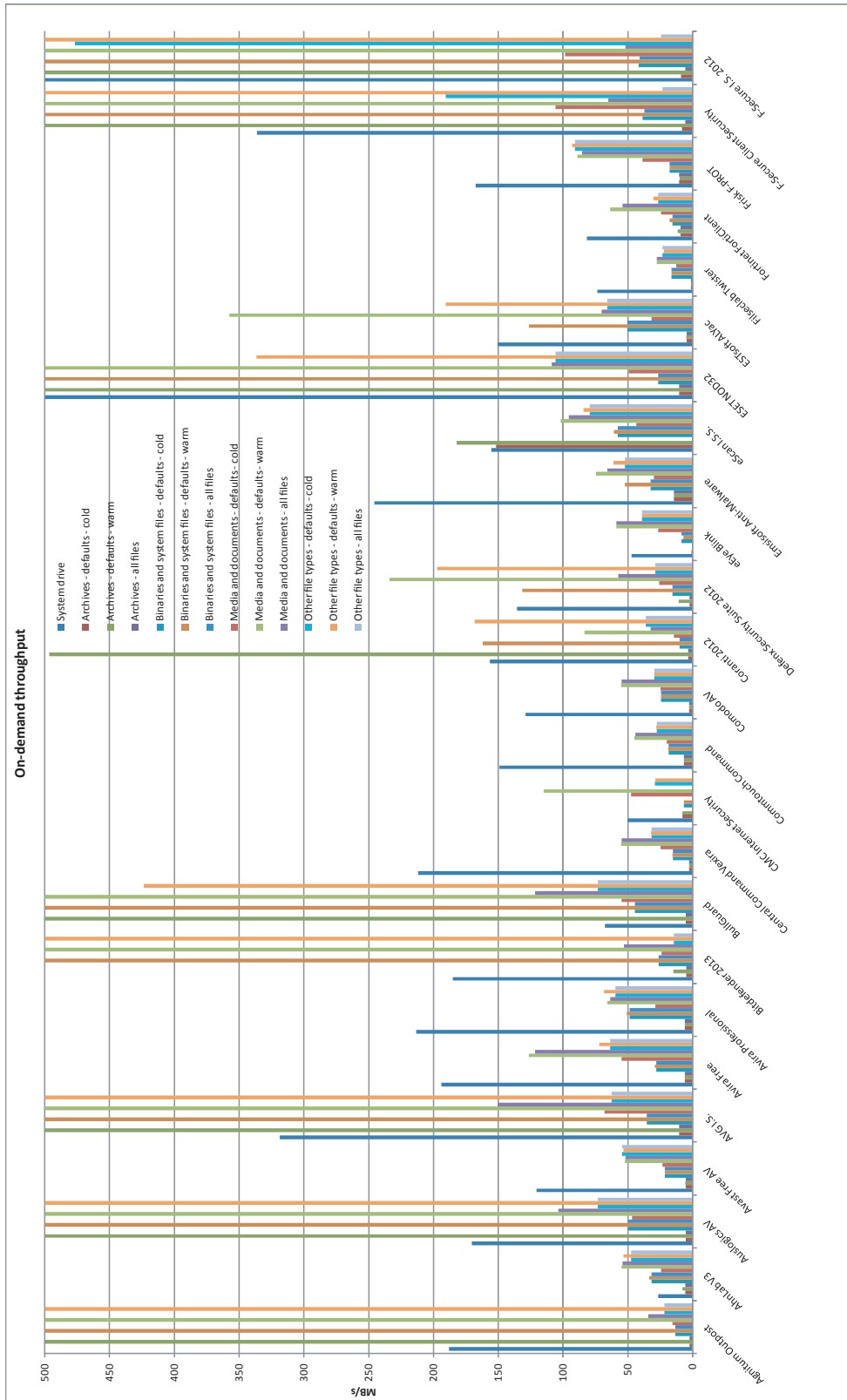
Please refer to text for full product names.

properly dealt with, in the clean sets, alongside a selection of warnings about suspicious and packed files, there was the same single FP on a file produced by *IBM*. This denies *Defenx* a VB100 award for the first time in a while – it stands on four passes and one fail in the last six tests; nine passes and one fail in the last two years with just the *Linux* tests not entered. The odd behaviour and slowdowns during the on-access measures were fairly intrusive but only occurred under heavy malware bombardment. No other issues were noted, so *Defenx* merits a 'Fair' rating for stability.

eEye Digital Security Blink Professional

Main version: 5.0.2, Rule version 1634
Update versions: 1.1.2173, 1.1.2204, 1.1.2215, 1.1.2222

ItW Std	99.84%	**ItW Std (o/a)**	99.84%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Blink is another product incorporating a third-party engine alongside in-house specialism (in this case the *Norman* engine with *eEye*'s vulnerability expertise), and *eEye* is another company involved in the spate of recent mergers and acquisitions, having been taken over by *BeyondTrust* at around the time of submissions for this comparative.

RAP 93.4%
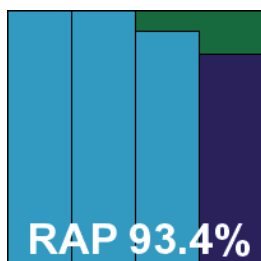
The product provided for testing was fairly sizeable at 242MB, and took some time to do its business, starting with a lengthy period of unpacking, preparation and installation of dependencies. After a few steps to click through, the process then ran for a couple of minutes before presenting a brief set-up wizard, finally opening its interface and offering to run an update. This final stage pulled down over 200MB of data on each install and took on average eight minutes to complete, making it one of the slowest this month, but no reboots were required.

The product interface is unflashy but clear and well presented, with a set of controls slightly more detailed than the most basic. Operation seemed smooth with no stability issues, and speed tests proceeded without hindrance. Apart, that is, from the product's inherent sluggishness – the scanning of binaries and particularly of archives taking an age to complete, even though it seemed only a single layer of nesting was being analysed. Overheads were pretty heavy, but RAM use was low, CPU use not too high, and our set of tasks at least managed to get through in good time.

Detection rates were impressive, continuing a steady improvement observed in recent months, and well up with the leading cluster in the RAP and Response tests. There were no issues in the clean sets, but in the WildList sets a single item was ignored both on demand and on access in all three test runs, thus denying *eEye* a VB100 award this month despite a generally decent showing. The vendor now has four passes and one fail from the last six tests, with the *Linux* test missed out; seven passes and two fails from nine attempts in the last two years. With no bugs or problems to report, the product earns a 'solid' stability rating.

Emsisoft Anti-Malware

Main version: 6.6.0.1
Update versions: 5,913,562; 5,952,590; 5,976,533; 6,001,549

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	99.93%	**ItW Extd (o/a)**	99.93%
False positives			0

There are more changes to report here, with *Emsisoft* announcing towards the end of testing that it would be changing the core engine in its future products from long-time partner *Ikarus* to the ever more prevalent *Bitdefender*; the switch will be accompanied by a major new release of the product. For one last look at it in its old form, we used a 134MB executable downloaded from the company's website, which included the latest updates available when fetched. Installation involves very few clicks, and zips through in a minute or so. At the end there are a few more steps to click through, including licensing and joining a community feedback scheme. Updates follow, pulling down close to 130MB of additional data but completing in only a couple of minutes.

RAP 95.4%
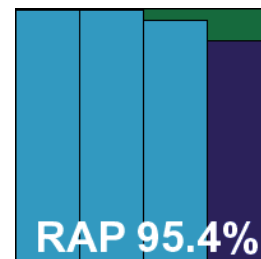
The product interface is slightly quirky but reasonably clear once you've got used to the odd behaviour of its menu panel, and it provides some basic configuration options. Logging is in a clear text format.

Operation was interrupted several times – in fact, just about every time a scan of malicious files was run – with error messages usually warning of a 'major problem'. In most cases this meant no further scans could be run and protection was disabled. Sometimes, simply rebooting solved the problem (although this on its own was rather

frustrating with lots of jobs to do), but in a number of instances the interface still refused to open after reboot and protection could not be restarted – so we had no choice but to wipe the test machine and start again as best we could.

With this extra work delaying things, it was fortunate that scanning speeds were zippy enough to recoup some lost time. Overheads were a little on the heavy side though, with low RAM use but fairly high CPU use and a lowish impact on our set of tasks. Detection rates were excellent in the RAP and Response sets – very close to the top of the field – but in the WildList sets a single item went undetected throughout the testing period, denying *Emsisoft* a VB100 award this month. The vendor's history shows one pass and four fails in the last six tests; two passes and eight fails in the last two years. With the severity of the issues noted mitigated by only having occurred during scans of large malware sets, their sheer frequency nevertheless merits a rating of 'buggy'.

eScan Internet Security Suite

Main version: 11.0.1139.1230

Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another product using a third-party engine, *eScan* is part of this month's crowded raft of *Bitdefender*-based solutions, with some additional
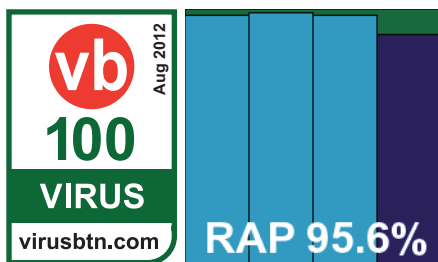
technology of its own on top. The installer measured 189MB, and did nothing too surprising during the set-up process, which took about a minute and ended with a reboot. Initial update times ranged from four to eight minutes, depending how far we were from the original submission date.

The interface has curvy corners and cute jumbo icons, but underneath there is a serious degree of fine-tuning available. Logging is clear, readable and reliable. Scanning speeds were very fast indeed, and overheads pretty light, but use of RAM was a little high and CPU use was through the roof; our set of tasks was completed in reasonable time though.

Moving onto the malware tests, initial attempts at on-access testing proved ineffective – nothing seemed to be picked

up at all. On rebooting the system, suddenly all was fine again. It appeared that for some reason two reboots were required, one after the initial install and a second after the first update, but this was not made clear by the product and users could easily think they were protected when they were not at all. This occurred on two of the three main test runs.

We also had some problems with the RAP tests taking rather a long time, which we suspected may have been due to failed attempts at cloud look-ups; the job ran through without errors, but took 60 hours (whereas the fastest products – including some using the same base engine – took less than two hours to do the same thing, with almost identical results). It was worth the wait though, as scores were splendid, putting *eScan* right up in the top corner of our RAP chart with its many relatives in the *Bitdefender* family. Response scores were splendid too, and with the WildList and clean sets handled well, a VB100 award is earned. That puts *eScan* on six passes in the last six tests; 11 passes and a single fail in the last two years. The product's stability was problematic on this occasion though, with some serious problems leaving the system unprotected. As a result, it earns a 'buggy' rating.
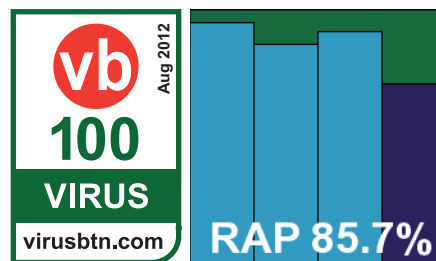
ESET NOD32 Antivirus 5

Main version: 5.2.9.1

Update versions: 7235, 7284, 7303, 7314

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Still maintaining an epic run of success in VB100 testing, *ESET*'s current product line has grown pretty familiar over the last few

years and rarely gives us much trouble. The build submitted this month measured a compact 50MB including all required data for the RAP tests. Installation was fairly simple if a little on the slow side, completing in around four minutes on average, but with very zippy update times adding only around 30 seconds. The interface is very slick and good-looking, and provides a wealth of configuration; logging is clear and reliable, with plenty of ways to export to text files.

Speed measures showed fast scanning speeds and light overheads, with resource use very low – especially CPU

use – but our set of tasks took a little longer than average. Detection rates were pretty good across the board, and with no issues in the certification sets *ESET* comfortably earns another VB100 award. The vendor remains on its extended run of success, with 12 passes in the last two years. A single GUI crash did occur during one of the RAP tests, but nothing was lost and no lasting damage was done, nevertheless it brought the product's rating down to just 'stable'.

ESTsoft ALYac Enterprise

Main version: 2.5.0.18

Update versions: 12.4.26.1/433901.2012061916/7.42659 /7309216.20120619, 12.4.26.1/436785.2012071117/7.43 864/7363079.20120710, 12.4.26.1/437480.2012071714/ 7.42897/7363560.20120715, 12.4.26.1/438143.2012072 313/7.42918/7360237.20120718

ItW Std	99.84%	**ItW Std (o/a)**	99.84%
ItW Extd	99.85%	**ItW Extd (o/a)**	99.80%
False positives			0

Another *Bitdefender*-based product, *ESTsoft*'s performances in our tests have been rather unpredictable so far, with some scores closely matching those of related solutions and others differing wildly. This month's installer measured 142MB, ran through the standard process and took around two minutes to do

RAP 92.8%

its actual work. No reboot was required to complete, and updates seemed more stable than we have observed in the past, the duration being hard to predict and ranging from three to 10 minutes in various runs.
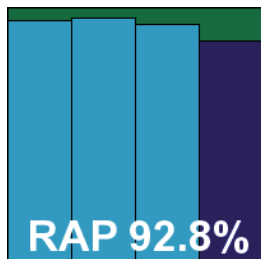
The interface is reasonably clear and usable, providing a limited set of controls; logging is decent, if rather slow to export and to save at the end of a scan. Scanning speeds were impressive though, and overheads fairly light, with low use of resources and a very low impact on our set of tasks.

Detection rates were superb in the RAP sets, but the Response scores were some way lower than expected, hinting that updating had not perhaps been as successful as it appeared. The clean sets were handled well, but in the WildList sets a small number of items were consistently ignored, which we could only ascribe to some additional whitelisting having gone awry. This denies *ESTsoft* a VB100 award this month, its first fail from four entries, all

in the last six tests. A minor issue was noted, in that options to adjust archive scanning appeared non-functional. This was counted as a trivial bug, but was enough to put the product in the 'stable' category.

Filseclab Twister Antivirus V7

Main version: 7.3.4.9985

Update versions: 15.160.27442, 15.188.60694, 15.198.24291, 15.206.2179

ItW Std	95.47%	**ItW Std (o/a)**	95.47%
ItW Extd	93.52%	**ItW Extd (o/a)**	92.32%
False positives			114

Still striving to reach its first VB100 award, *Filseclab* continues to enter our tests regularly. The product was downloaded from the vendor's public website, coming as a main installer and an update bundle each measuring just over 130MB. The install process only requires a couple of clicks and completes

FP 8
RAP 88.3%

in under a minute; online updates added another few minutes to the total, and a reboot was required to complete the job.
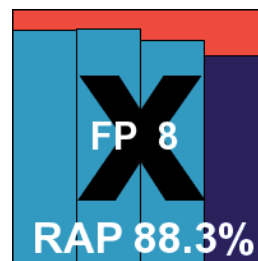
The interface is unusual but reasonably well presented, providing a little more than the bare minimum of controls, once they have been found amongst the rather wordy layout. Things seemed to run fairly smoothly throughout, with no bugs or issues observed. Speeds were pretty sluggish though, and lag times fairly high too, although our set of tasks completed in reasonable time and resource use was within normal limits.

Detection was pretty reasonable in the RAP and Response sets, although in the WildList sets there were still a few misses, with gradual improvement over the course of the three main test runs. False positives also remain a problem, with the large numbers this month mostly down to separate detection of numerous items in the *Cygwin* package, included on a *Netgear* drivers CD. Other packages alerted on included several from *Adobe*, with *Microsoft*, *Google*, *IBM*, *Sun/Oracle* and *SAP* among other providers whose files were labelled as malicious.

So, there can be no question of *Filseclab* winning a VB100 award this month, leaving the vendor with no passes from three tries in the last six tests; five fails in the last two years, but stability at least was good, earning the product a 'solid' rating.
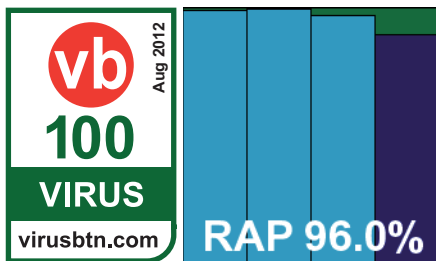
Fortinet FortiClient

Main version: 4.1.3.149

Update versions: 5.0.21/15.724, 15.809, 15.866, 15.886

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another product which has shown strong improvement in our RAP tests of late, *Fortinet* returns doubtless hoping for more of the same. The installer is very small at less than 10MB, with an update bundle measuring 143MB provided for offline use. Set-up runs through rapidly with minimal fuss and no need to reboot, and updates are speedy, the whole process taking little more than a couple of minutes.

The interface is plain and businesslike, providing a very thorough set of controls, and logging is clear, reliable and easy to read. Scanning speeds were a little below average, overheads a little heavy on access; RAM use was also around average, CPU use very low, but our set of tasks took a long time to complete. Detection rates were very impressive though, continuing the recent upward trend, and with no issues in the certification sets a VB100 award is comfortably earned.

With no participation in our *Linux* tests, *Fortinet* now has five passes from five entries in the last six tests; nine passes and a single fail in the last two years. A single issue was noted: one of the Response test scans bailed out with a message that it had been 'interrupted'. There was no apparent loss of protection though, and the same job completed without any problems on a second attempt, meaning a 'stable' rating is merited.

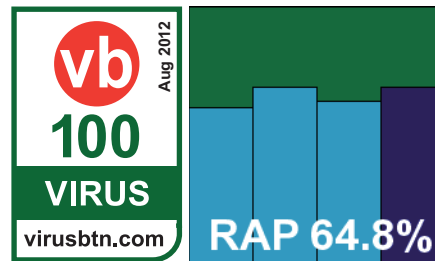## Frisk Software F-PROT Antivirus for Windows

Main version: 6.0.9.6

Update versions: 4.6.5/19/06/2012, 23:32; 11/07/2012, 14:11; 16/07/2012, 23:37; 23/07/2012, 13:25

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	98.85%
False positives			0

Frisk has been involved in one of the big industry events of recent months with its acquisition by *Commtouch*. However, it seems the *Frisk* product lines will continue to operate as usual (for the time being at least), with a major new version due out fairly soon. The current product remains familiar from many years of testing, with the installer a compact 35MB and updates measuring 58MB. Set-up is quick and easy, completing in around a minute with a reboot required; updates add another couple of minutes to the total time taken.

The interface is plain and simple, providing basic controls only, but logging is clear and dependable and operation was generally smooth. After part of the RAP tests the interface refused to run any more scans, the browse-for-folder dialog simply disappearing as soon as it opened, but a reboot resolved this without too much pain. Scanning speeds were decent, overheads perhaps a little above average in some areas (mainly the set of binaries), but our set of tasks ran through rapidly, with low memory consumption and CPU use just a little above average.

Detection rates were not too impressive, but at least fairly consistent, and the core sets were properly dealt with, earning a VB100 award for *Frisk*; the vendor can boast a clean sheet of six passes in the last six tests; ten passes and two fails in the last two years. With a single GUI issue occurring under heavy pressure, a 'stable' rating is also earned.
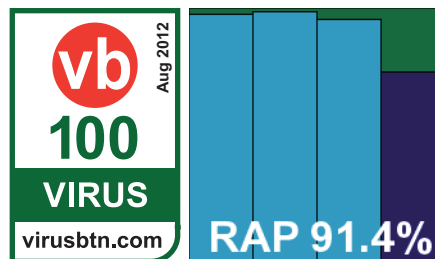
F-Secure Client Security

Main version: 9.31 build 118

Update versions: 9.30 build 17464

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	95.92%
False positives			0

A brace of products were submitted by *F-Secure* as usual, adding further to the lengthy list of solutions that include

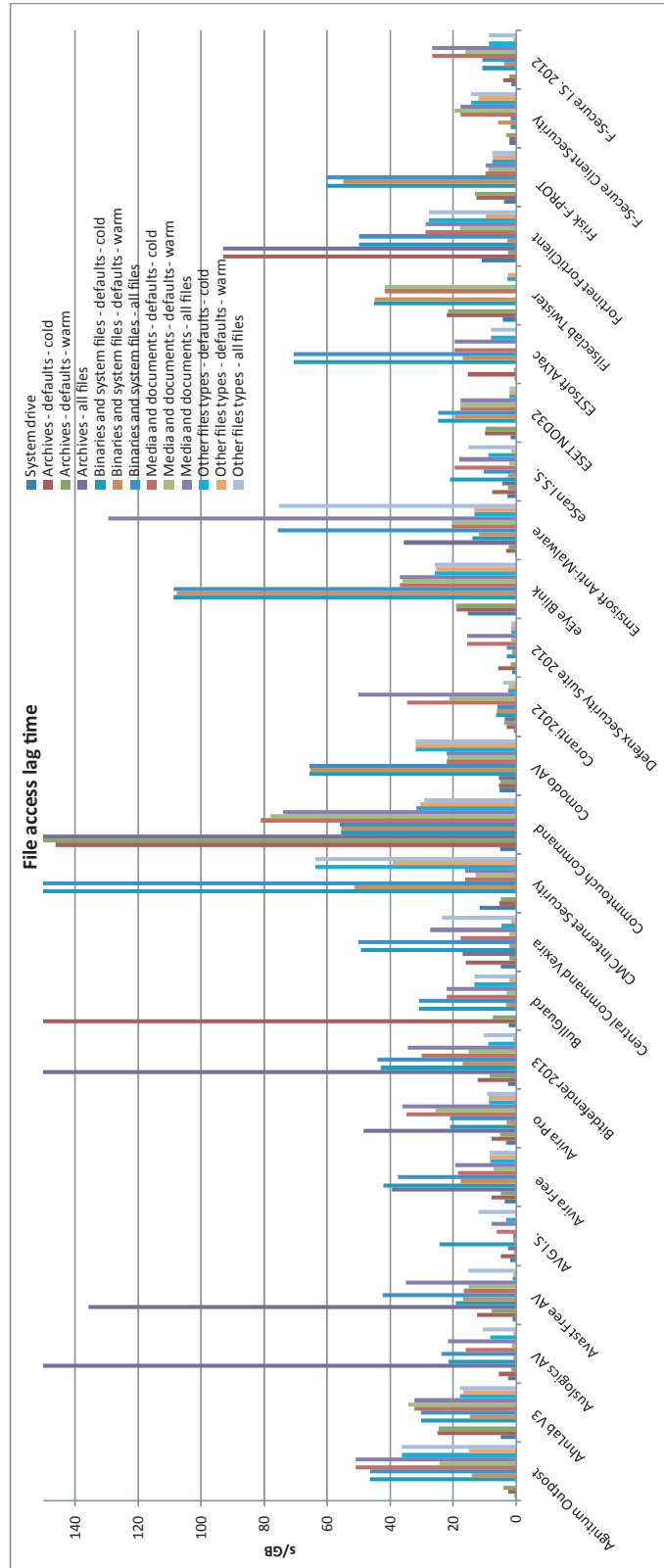| File access lag time (s/GB)	System drive*	Archive files			Binaries and System files			Media and Documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost	0.37	2.59	4.04	NA	46.32	13.96	46.32	50.85	24.26	50.85	36.24	14.90	36.24
AhnLab V3	4.92	24.93	24.57	NA	30.15	14.75	30.15	32.20	34.20	32.20	17.93	16.75	17.93
Auslogics Antivirus	2.62	5.51	1.46	163.49	21.39	0.81	23.63	15.95	1.37	21.54	8.18	0.78	10.49
Avast Free Antivirus	1.07	12.35	7.80	135.74	19.07	16.85	42.30	16.58	15.08	35.05	1.09	0.80	15.06
AVG Internet Security	1.94	4.74	0.56	2.45	24.23	0.79	0.96	6.17	0.18	7.86	3.07	0.10	11.89
Avira Free Antivirus	3.58	7.80	4.85	39.46	42.13	17.56	37.50	18.46	7.14	19.26	8.15	8.36	8.33
Avira Pro Security	3.15	7.81	4.99	48.51	20.90	2.91	20.93	34.72	25.56	35.98	8.64	8.57	9.25
Bitdefender AV Plus	2.54	12.25	8.31	174.24	43.05	17.04	44.10	30.01	15.06	34.33	8.78	0.90	10.38
BullGuard	2.22	197.36	7.32	NA	30.80	3.19	30.80	21.95	2.85	21.95	13.23	2.17	13.23
Central Command Vexira	4.80	15.85	2.05	17.07	49.21	2.06	50.18	17.63	2.17	27.22	4.57	1.52	23.51
CMC Internet Security	11.45	5.17	4.86	NA	176.71	51.33	176.71	16.16	12.88	16.16	63.72	39.13	63.72
Commtouch Command	5.11	146.31	153.67	165.52	55.65	55.59	55.94	81.19	77.87	73.99	31.75	30.31	29.15
Comodo Antivirus	5.35	5.47	5.06	5.47	65.57	65.40	65.57	21.99	21.81	21.99	31.77	31.91	31.77
Coranti 2012	0.70	3.05	3.76	3.60	6.30	6.01	5.94	34.63	21.20	50.10	2.52	2.26	4.02
Defenx Security Suite	1.35	5.59	1.71	NA	2.88	1.31	2.88	15.62	1.53	15.62	1.41	1.46	1.41
eEye Blink Professional	15.26	18.85	19.11	NA	108.68	107.73	108.68	36.79	35.99	36.79	25.88	25.30	25.88
Emsisoft Anti-Malware	0.00	3.25	2.38	35.68	13.81	11.82	75.68	20.41	20.14	129.58	13.20	13.22	75.28
eScan I.S.S.	2.68	7.54	2.51	4.39	21.02	2.48	10.22	19.44	2.17	18.03	8.89	1.53	15.04
ESET NOD32	1.67	9.85	9.66	NA	24.82	19.50	24.82	17.60	17.64	17.60	2.18	2.09	2.18
ESTsoft ALYac	0.53	15.38	0.59	NA	70.57	16.99	70.57	19.42	0.29	19.42	8.03	0.08	8.03
Filseclab Twister AV V7	4.29	21.98	21.57	NA	45.03	44.78	NA	41.75	41.72	NA	2.66	2.64	NA
Fortinet FortiClient	10.90	93.15	2.53	93.15	49.97	2.68	49.97	28.81	17.86	28.81	27.58	9.64	27.58
Frisk F-PROT Antivirus	3.69	12.61	13.04	NA	60.37	54.97	60.37	9.69	8.78	9.69	7.59	7.39	7.59
F-Secure Client Security	2.19	2.04	3.18	NA	1.77	5.60	1.77	17.58	19.45	17.58	14.30	11.96	14.30
F-Secure I.S. 2012	1.57	3.94	2.06	NA	10.63	3.75	10.63	26.54	16.06	26.54	8.67	0.79	8.67
G Data AntiVirus 2013	1.66	76.72	4.33	243.17	62.78	14.78	23.00	55.76	24.55	38.59	32.53	15.49	21.74

System drive size measured before product installation.
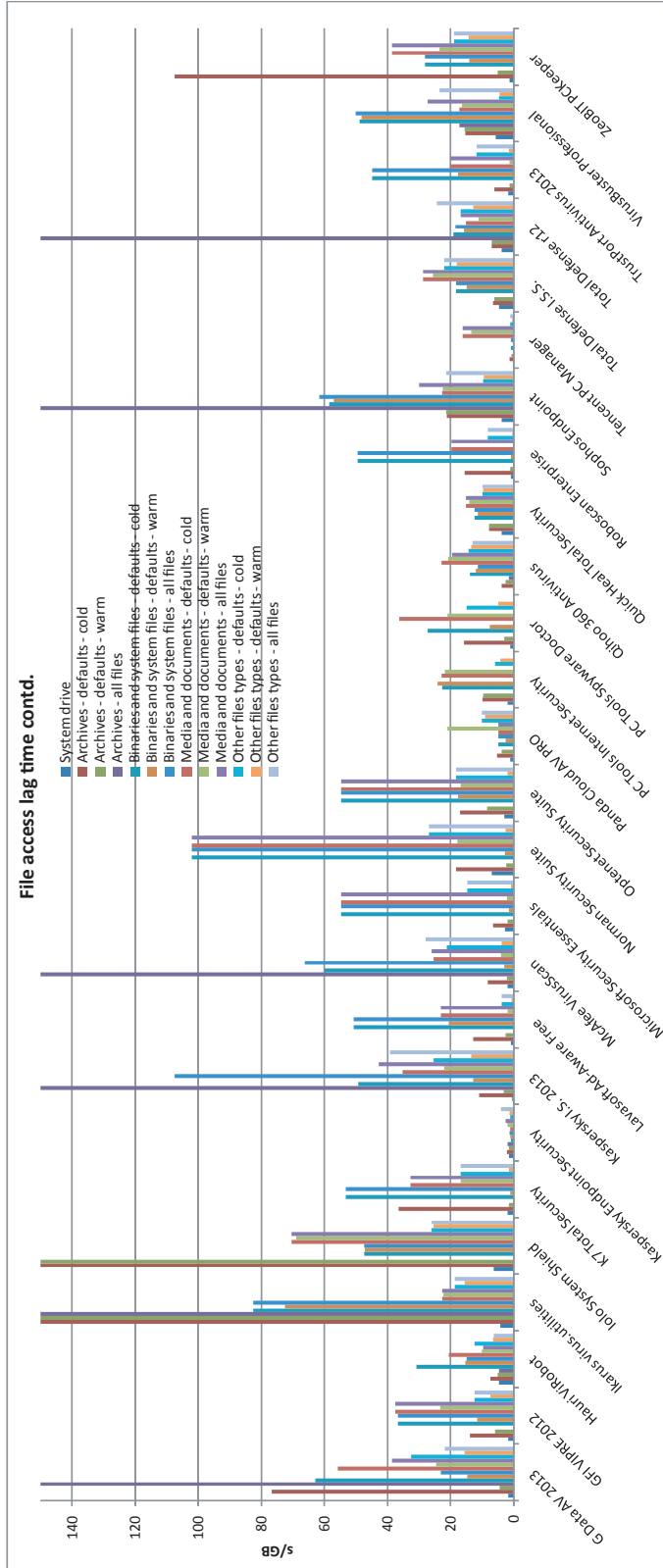
Please refer to text for full product names.

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
GFI VIPRE Antivirus	1.73	13.91	5.95	NA	36.61	11.64	36.61	37.52	23.23	37.52	12.35	7.33	12.35
Hauri ViRobot I.S.	4.69	7.32	5.04	4.65	30.81	15.27	15.00	20.61	10.18	9.66	12.32	6.56	6.34
Ikarus virus.utilities	4.15	188.23	188.57	188.23	82.52	72.46	82.52	22.65	22.15	22.65	18.57	15.47	18.57
Iolo System Shield	6.31	158.20	163.42	NA	47.35	47.17	47.35	70.49	68.86	70.49	25.96	25.42	25.96
K7 Total Security	1.82	36.43	1.42	NA	53.17	1.04	53.17	32.73	16.68	32.73	16.87	1.48	16.87
Kaspersky E.S.	1.49	2.08	1.56	1.84	0.90	1.10	1.35	1.11	1.85	2.59	1.06	1.27	4.05
Kaspersky I.S.	0.49	11.00	3.25	219.56	49.17	12.85	107.51	35.23	21.93	42.83	25.34	13.44	39.22
Lavasoft Ad-Aware	0.92	12.82	2.62	NA	50.68	20.52	50.68	22.98	1.82	22.98	3.86	0.61	3.86
McAfee VirusScan	1.87	8.14	2.16	387.10	59.95	2.97	66.28	25.40	3.95	26.05	21.10	3.69	27.82
Microsoft S.E.	2.83	6.44	1.93	NA	54.63	1.41	54.63	54.63	2.13	54.63	14.64	0.83	14.64
Norman Security Suite	6.90	18.27	2.32	NA	102.08	2.72	102.08	102.08	17.78	102.08	26.87	2.44	26.87
Optenet Security Suite	2.94	16.94	8.37	NA	54.61	17.70	54.61	54.61	16.74	54.61	18.19	1.87	18.19
Panda Cloud AV PRO	1.17	5.32	3.84	NA	4.76	2.46	4.76	4.76	20.91	4.76	10.14	9.09	10.14
PC Tools I.S.	1.97	9.77	9.73	NA	22.68	24.14	NA	22.91	21.82	NA	5.94	4.22	NA
PC Tools S.D	1.00	15.75	2.87	NA	27.30	7.61	NA	36.30	21.05	NA	14.86	4.85	NA
Qihoo 360 Antivirus	0.00	3.80	2.43	1.53	13.94	11.86	11.37	22.90	20.84	19.56	14.20	13.53	13.08
Quick Heal TS 2012	3.82	7.83	7.79	NA	12.34	11.29	12.34	15.09	14.05	15.09	9.93	9.66	9.93
Roboscan Enterprise	0.88	15.47	1.13	NA	49.48	0.87	49.48	19.81	0.11	19.81	8.10	0.51	8.10
Sophos E.S.C.	3.70	21.16	21.45	372.84	58.52	57.09	61.63	22.57	22.37	30.00	9.62	9.48	21.43
Tencent PC Manager	0.15	1.30	0.69	NA	0.84	0.24	0.84	16.26	13.36	16.26	1.11	0.36	1.11
Total Defense I.S.S.	4.69	6.43	6.07	NA	18.24	14.92	18.24	28.70	25.59	28.70	21.97	18.13	21.97
Total Defense T.D. r12	3.74	6.99	6.84	252.14	19.15	15.71	18.52	15.12	11.18	16.68	16.71	12.76	24.36
TrustPort Antivirus	1.61	6.19	1.28	NA	44.97	17.53	44.97	20.23	1.30	20.23	11.82	1.57	11.82
VirusBuster Professional	5.66	15.25	15.47	17.13	48.76	48.19	50.08	17.16	16.39	27.16	4.61	4.41	23.43
ZeoBIT PCKeeper	1.33	107.44	5.02	NA	28.08	14.10	28.08	38.56	23.39	38.56	18.79	14.32	18.79

System drive size measured before product installation.

Please refer to text for full product names.

File access lag time

Please refer to text for full product names.

File access lag time contd.

Legend:
- System drive
- Archives - defaults - cold
- Archives - defaults - warm
- Archives - all files
- Binaries and system files - defaults - cold
- Binaries and system files - defaults - warm
- Binaries and system files - all files
- Media and documents - defaults - cold
- Media and documents - defaults - warm
- Media and documents - all files
- Other files types - defaults - cold
- Other files types - defaults - warm
- Other files types - all files

y-axis: s/GB

Categories: G Data AV 2013, GFI VIPRE 2012, Hauri ViRobot, Ikarus virus.utilities, Iolo System Shield, K7 TotalSecurity, Kaspersky Endpoint Security, Kaspersky IS 2013, Lavasoft Ad-Aware Free, McAfee VirusScan, Microsoft Security Essentials, Norman Security Suite, Optenet Security Suite, Panda Cloud AV PRO, PC Tools Internet Security, PC Tools Spyware Doctor, Qihoo 360 Antivirus, Quick Heal Total Security, Roboscan Enterprise, Sophos Endpoint, Tencent PC Manager, Total Defense 1.5.5, Total Defense r12, Trustport Antivirus 2013, VirusBuster Professional, ZeoBIT PCKeeper

Please refer to text for full product names.

the *Bitdefender* engine, although in this case a little more in-house work is incorporated than in most. Set-up was fairly straightforward, with options related to management systems indicating that this is *F-Secure*'s corporate product line. The process took a couple of minutes with no need to reboot; update times were harder to measure, as the process would start, claim it had run, but in fact downloading and installation of new data continued in the background for some time. In some cases we couldn't be sure the product was fully ready for testing for around 20 minutes.

Speed measures ran smoothly, showing some good times to start with and huge speed-ups in the warm runs; overheads were also light, with RAM and particularly CPU use quite low; our set of activities did take a while to complete, but not excessively so.

Moving onto the malware tests, things got a little more problematic. In the RAP runs, on several occasions logs were truncated, missing vital detail; repeating the runs several times was necessary to ensure we gathered a full set of figures. Even so, with the score for the proactive week lower than expected, it remains possible that some data was lost. Moving onto the Response and certification tests, the first run hit a nasty snag. An initial attempt to run an on-access job over the WildList sets froze up completely around 2% of the way through. After rebooting and retrying, it seemed to run better, but looking at the logs it was clear that all was still not right. Chunks of files were ignored, hinting that detection was shutting down for periods before being re-enabled. The test was re-run multiple times, but comparing results showed identical patterns each time, so it would seem that some samples were tripping the scanner up, causing it to stop working until it could fix itself. On later runs these problems were not apparent, and much work providing debug information to the developers has yet to pin down the cause of the issue.

In the end, detection rates were very good, especially in the Response sets, with RAP scores possibly hit by logging issues. The WildLists were well covered in most runs, and in the one instance where things went horribly wrong, only the Extended list was affected; as we currently only require on-demand coverage of this set, which was well provided, *F-Secure* earns a VB100 award for this product by the very skin of its teeth. The test history for the company's mainline product now shows three passes and one fail from four entries in the last six tests; eight passes and one fail in the last two years. The problems noted in one of the test runs did not recur in later runs, but were repeatable at the time and resulted in temporary loss of protection; on top of the logging issues, this pushes the product into the 'buggy' category.

F-Secure Internet Security 2012

Main version: 12.56 build 100
Update versions: 10.00 build 18110

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The second product from *F-Secure* was a little different this month. Due to its install method, and some delay with the developers' initial decision to submit it, it was not possible to include it in the RAP tests. The package sent to us was a tiny 1MB downloader tool, which when run fetched the main component, installing a 'launch pad' utility which would then be used to control other components, including the 'computer security' item of which the anti-malware product was a sub-component. Initial attempts to follow this process proved difficult though, as once the launch pad was in place, attempting to install the security part from it repeatedly hit a wall; licence details were requested, but once provided a message abruptly stated that the service was unavailable and that we should try again later. After several attempts with a number of licence keys, with the help of the developers we finally managed to get to the bottom of the problem, which involved certification keys that had not been updated as the installation of *Windows* was new and had not yet been online very much. As we would recommend people install security solutions as early as possible in their computer's lifecycle, this seems less than ideal (as indeed does the idea of a product which can only be installed from the web).

Eventually, after several days of trying, we finally managed to get a working product, and from there things moved along much more smoothly. The issues observed with the other *F-Secure* solution were not encountered, but it is of course possible that this may have something to do with the delay in getting under way; we try to ensure that similar products are run as closely together as possible, but if the issues affecting the other product were caused by some faulty updates or engine problems, it's possible that this product would also have been affected, had we tested it on the same day (as intended).

As it was, speed tests were zippy, especially in the warm runs, and overheads light, with medium RAM use, low CPU use and a fairly high impact on our set of activities. Detection rates were excellent in the Response sets, with no RAP scores for comparison, and the core sets were well handled, earning another VB100 award for *F-Secure*,

this time a lot more comfortably. We haven't seen a second product from *F-Secure* in a while, the company's submission patterns playing havoc with our system of categorizing products, but with this one in the *I.S.* line we have only seen this single entry in the last six tests; three passes from three entries in the last two years. The initial install issues were intentional but still a minor annoyance, and with a single instance of inaccurate logging too, the product falls into the 'stable' category.

G Data AntiVirus 2013

Main version: 23.0.3.2
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Yet another product incorporating *Bitdefender*'s hugely popular engine, this time with additional contributions from *Avast*,
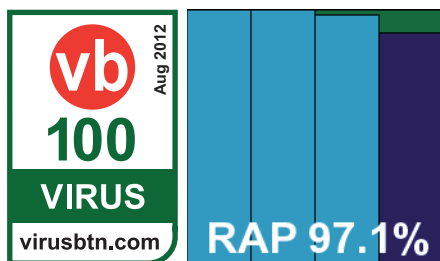
G Data is one of our most consistently strong performers. The build entered this month measured 235MB including its updates, but installation was speedy and simple with just a handful of clicks, and a reboot was needed at the end. Updates were fairly zippy too, rarely taking more than two minutes to complete.

The interface looks good and provides excellent configuration; logging is also clear and easy to use. Scanning speeds were a little sluggish initially but powered through the warm runs in no time; file access lags were rather high, again improving greatly after an initial familiarization period, and resource use was low, although our set of activities took a very long time to complete.

Detection rates were extremely impressive, close to perfect in some areas – this was one of very few products to break the 90% barrier in the proactive week of the RAP sets. The certification sets were brushed aside effortlessly, comfortably earning the product a VB100 award, and *G Data* now stands at five passes from five attempts in the last six tests; nine passes and a single fail from ten entries in the last two years. Stability was rated 'solid', verging on the 'indestructible'.

GFI VIPRE Antivirus 2012

Main version: 5.2.5162
Update versions: 12083, 3.9.2540.2/12215, 3.9.2542.2/12260, 3.9.2542.2/12338

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	99.90%	**ItW Extd (o/a)**	99.90%
False positives			0

GFI has put in some consistently decent performances of late, but we still occasionally see issues handling large sets of malware, caused by an inefficient logging system which keeps all data in memory rather than the more standard approach of using a log file. The current version comes as a 116MB installer with 85MB of data provided for the RAP tests. It was set up with a minimum of interaction, completing in a couple of minutes with no need to reboot. Updates were fairly zippy, the longest taking just over three minutes, and the interface is bright and shiny, providing not much beyond the basic controls required. Logging is rather unfriendly for the human reader, but parsing tools provided by the vendor have proved very helpful.
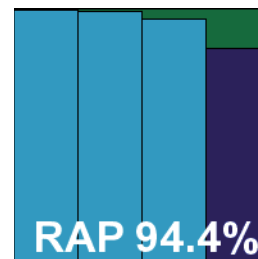
Scanning speeds were pretty sluggish, overheads perhaps a little on the high side, but resource use was low and our set of tasks completed in good time. Detection rates were mostly excellent, as long as we didn't try to scan too much at once, in which case scans routinely stopped abruptly, leaving no usable data behind. This would be unlikely to affect the normal user though, and it was not too difficult to gather full data for the RAP and Response tests. The core sets were again fiddly thanks to a lack of usable logging of on-access activities and a rather quirky approach to some samples – to which access is initially allowed, but which are later removed once some background scanning has completed.

The clean sets were handled OK, but on looking over the WildList results we saw that a handful of items in the Extended List had been missed on the third and final run, both on demand and on access. Further investigation and consultation with the developers revealed that this was due to an error with a set of updates – which had been fixed promptly. The timing of our test was a little unfortunate, as running it a few hours earlier or later would probably have avoided the issue. Nevertheless, no VB100 award can be granted this month, despite a clean sheet in two of the three runs. *GFI* now has three passes and two fails in the last six

Response tests	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
Agnitum Outpost	85.79%	81.96%	79.94%	80.17%	83.73%	82.04%	67.66%	80.18%
AhnLab V3	95.48%	95.98%	95.39%	94.02%	93.85%	93.41%	92.44%	94.37%
Auslogics Antivirus	98.82%	99.01%	98.57%	98.91%	99.18%	98.70%	98.20%	98.77%
Avast Free Antivirus	99.30%	98.54%	98.67%	98.02%	98.62%	98.91%	93.82%	97.98%
AVG Internet Security	97.59%	97.92%	97.08%	97.68%	97.72%	98.14%	92.46%	96.94%
Avira Free Antivirus	99.71%	99.66%	99.66%	99.51%	99.58%	99.65%	99.51%	99.61%
Avira Professional Security	99.71%	99.66%	99.66%	99.51%	99.58%	99.65%	99.51%	99.61%
Bitdefender Antivirus Plus 2012	98.80%	99.00%	98.57%	98.90%	99.18%	98.68%	98.19%	98.76%
BullGuard	98.82%	99.02%	98.57%	98.91%	99.18%	98.70%	97.91%	98.73%
Central Command Vexira	85.01%	81.50%	80.94%	79.89%	83.26%	81.74%	67.52%	79.98%
CMC Internet Security	49.15%	70.67%	52.15%	79.37%	60.07%	58.43%	58.16%	61.14%
Commtouch Command Anti-Malware	95.93%	95.40%	91.32%	92.82%	90.92%	84.96%	82.72%	90.58%
Comodo Antivirus	93.70%	96.57%	96.63%	95.15%	95.85%	94.03%	93.85%	95.11%
Coranti 2012	99.17%	99.54%	99.12%	99.45%	99.54%	99.34%	98.67%	99.26%
Defenx Security Suite 2012	85.69%	81.92%	79.89%	80.13%	83.71%	81.75%	67.64%	80.10%
eEye Blink Professional	98.83%	99.14%	98.81%	98.77%	99.21%	98.53%	97.17%	98.63%
Emsisoft Anti-Malware	99.67%	99.74%	99.55%	99.59%	99.62%	99.52%	99.34%	99.58%
eScan Internet Security Suite	98.80%	99.02%	98.54%	98.93%	99.14%	98.66%	98.19%	98.76%
ESET NOD32 Antivirus 5	97.86%	96.43%	97.17%	96.36%	96.58%	96.89%	92.31%	96.23%
ESTsoft ALYac Enterprise	80.33%	87.63%	78.78%	84.26%	86.77%	70.84%	70.13%	79.82%
Filseclab Twister Antivirus V7	89.89%	92.46%	93.27%	93.43%	89.74%	93.15%	91.14%	91.87%
Fortinet FortiClient	99.24%	99.10%	98.83%	98.81%	98.76%	98.77%	96.06%	98.51%
Frisk F-PROT Antivirus	78.77%	77.69%	75.81%	74.51%	81.44%	69.64%	69.16%	75.29%
F-Secure Client Security	99.07%	99.27%	98.98%	99.17%	99.36%	98.98%	98.45%	99.04%
F-Secure Internet Security 2012	99.05%	99.10%	99.06%	99.24%	98.85%	99.13%	98.41%	98.97%
G Data AntiVirus 2013	99.69%	99.80%	99.77%	99.82%	99.82%	99.62%	99.51%	99.72%

Please refer to text for full product names.

Response tests contd.	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
GFI VIPRE Antivirus 2012	98.89%	99.32%	99.23%	99.48%	99.18%	97.99%	98.73%	98.98%
Hauri ViRobot Internet Security 2011	81.91%	89.55%	80.53%	86.29%	87.89%	71.97%	71.90%	81.43%
Ikarus virus.utilities	99.45%	99.70%	99.60%	99.61%	99.32%	99.61%	99.34%	99.52%
Iolo System Shield	71.08%	69.52%	67.84%	67.24%	72.81%	62.24%	61.28%	67.43%
K7 Total Security	94.71%	96.81%	93.55%	91.48%	93.75%	95.04%	85.28%	92.94%
Kaspersky Endpoint Security	97.69%	97.48%	97.41%	97.74%	98.54%	98.81%	97.44%	97.87%
Kaspersky Internet Security 2013	98.22%	98.12%	97.76%	98.28%	98.64%	98.97%	97.87%	98.27%
Lavasoft Ad-Aware Free Antivirus +	98.89%	99.32%	99.23%	99.48%	99.18%	97.99%	98.73%	98.98%
McAfee VirusScan Enterprise	91.12%	90.83%	88.92%	85.15%	91.78%	88.33%	86.91%	89.01%
Microsoft Security Essentials	90.41%	92.18%	91.14%	93.38%	94.36%	95.32%	89.62%	92.34%
Norman Security Suite	98.87%	99.16%	98.87%	98.81%	99.21%	98.58%	97.20%	98.67%
Optenet Security Suite	90.15%	87.94%	86.93%	88.25%	90.63%	90.02%	89.87%	89.11%
Panda Cloud Antivirus PRO	99.14%	99.80%	99.26%	99.14%	99.39%	99.55%	98.53%	99.26%
PC Tools Internet Security	97.06%	91.61%	87.95%	88.95%	85.57%	74.49%	92.97%	88.37%
PC Tools Spyware Doctor	97.12%	91.23%	87.81%	88.83%	85.69%	74.71%	92.86%	88.32%
Qihoo 360 Antivirus	98.00%	97.88%	97.61%	97.43%	98.66%	96.79%	95.88%	97.46%
Quick Heal Total Security 2012	83.02%	90.22%	82.65%	77.32%	86.70%	89.28%	67.08%	82.33%
Roboscan Enterprise Solution	80.33%	87.63%	78.78%	84.26%	86.77%	70.84%	70.13%	79.82%
Sophos Endpoint Security and Control	98.22%	99.57%	98.17%	99.41%	98.44%	97.76%	98.54%	98.59%
Tencent PC Manager	85.28%	90.97%	89.82%	88.22%	92.13%	91.08%	91.39%	89.84%
Total Defense Inc. Internet Security Suite	95.91%	95.70%	90.16%	92.11%	86.64%	87.67%	70.46%	88.38%
Total Defense Inc. Total Defense r12	63.78%	55.96%	61.07%	67.03%	56.37%	62.11%	48.31%	59.23%
TrustPort Antivirus 2013	98.70%	98.88%	98.42%	98.91%	99.07%	98.56%	98.14%	98.67%
VirusBuster Professional	85.45%	81.68%	81.16%	79.72%	83.29%	81.86%	67.52%	80.10%
ZeoBIT PCKeeper	99.76%	99.66%	99.68%	99.51%	99.61%	99.65%	99.51%	99.62%

Please refer to text for full product names.

tests; seven passes and three fails in the last two years. A few scans falling over when overloaded with detections were the only issues noted, earning the product a 'stable' rating.

Hauri ViRobot Internet Security 2011

Main version: 6.0.0.0
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Back to another *Bitdefender*-based product, *Hauri*'s *ViRobot* has been around for a long time and has seen something of a resurgence

vb 100 VIRUS virusbtn.com   Aug 2012   RAP 95.6%
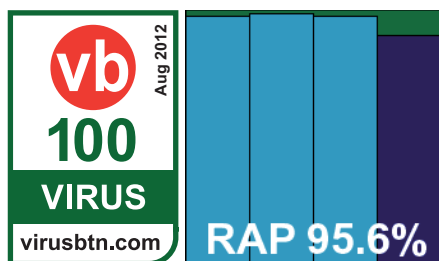
in our tests of late thanks to the vendor's partnership with external engine developers. The product was submitted as a 182MB installer including required updates, and installation ran through the standard set of steps with no reboot required. Updates were a little baffling at times, with the actual process running for no more than a couple of minutes, but on most occasions no apparent change was made to the information displayed on the product GUI; despite reassuring messages about the update having completed successfully, the version dates on the main interface rarely changed. However, after completing our standard process of attempting updates before and after a reboot, we had no choice but to continue with what we had.

The interface is fairly pleasant and easy to operate, with a decent level of controls, and logging is usable too, with a viewer utility and an easy method of exporting to file. Scanning speeds were slow, but overheads not too high; RAM use was low, but CPU use way up, and our set of activities took a little longer than average to complete.

Detection rates were superb in the RAP sets as expected, but in the Response sets they were rather lower than we might have predicted, hinting that perhaps the update process was not as successful as it claimed. There were no issues in the core sets though, so a VB100 award is earned, putting *Hauri* on two passes and one fail from three entries in the last six tests; two passes and four fails in the last two years. With updates clearly not fully reliable, and some issues noted starting up the on-access component, the product falls into the 'buggy' category this month.

Ikarus virus.utilities

Main version: 2.0.125
Update versions: 1.1.118/81544, 2.0.134/1.1.122/81704, 2.0.134/1.1.122/81777, 2.0.134/1.1.122/81825

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	99.93%	**ItW Extd (o/a)**	99.93%
False positives			0

Ikarus tends to have rather uneven luck in our comparatives, and another appearance from its engine in this test hints that a recent spell of good fortune may have come to an end. The product submitted came as an ISO image of an install CD with many additional components, the whole thing measuring 204MB,

RAP 95.5%

while updates came as a separate bundle of 82MB. Set-up is simple and direct, with the standard path followed, although options to join a feedback scheme appeared to be hidden, greyed-out by default, alongside the normal update settings. The product interface can be a little slow to open, especially on first run, but updates were mostly fairly zippy, taking a couple of minutes to complete. On one occasion an update failed, with an error message displayed in German. However, the GUI informed us that the last update had been a minute or so previously – which one might be forgiven for thinking meant last *successful* update, rather than merely the last update *attempt*. Rebooting and retrying resolved the issue easily though.
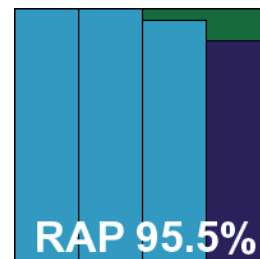
The GUI is pretty perfunctory, providing the bare minimum of controls, but it seems to have become much more stable of late, running well for most of the tests. After some of the speed tests it did get a little tangled up in itself though, refusing to start any more scans, and once again a reboot was needed to return things to normal. Scanning speeds were pretty slow for the most part, a little better over our sets of media and miscellaneous files than over executables and archives. On-access lag times were very heavy indeed. RAM use was low, but CPU use rather high, and our set of tasks ran through very quickly. Logging was clear and reliable throughout.

Detection rates were excellent in the RAP and Response sets, with a handful of items in the clean sets marked as suspect thanks to embedded scripts. The WildList sets were mostly well dealt with, but a couple of items in the Extended set were ignored, meaning no VB100 award for *Ikarus*, as expected. The vendor now has two passes and two fails in the last six tests; three passes and five fails

in the last two years. A few issues with the updater and scanner mean only a 'fair' rating for stability.

Iolo System Shield

Main version: 4.2.11.0
Update versions: NA

ItW Std	99.20%	**ItW Std (o/a)**	100.00%
ItW Extd	98.40%	**ItW Extd (o/a)**	100.00%
False positives			0

In something of a surprise move, *Iolo*'s developers informed us this month that they would like their product to be omitted from the RAP test. Having made participation in the RAP tests optional so as not to unfairly represent products that require access to cloud data to function properly, this was the first time a product had been withdrawn from the test for other reasons (the developers cited poor performances in previous tests) and has made us question whether such a move should be permitted. It is likely that the rules will be tightened when we complete a redraft of the official procedures documents, currently under way.

As far as testing goes it made things much easier of course, as *Iolo*'s product has never been the easiest to work with. The installer submitted was a tiny 500KB downloader, which on first operation fetched the main installer, measuring 55MB. An option is usefully provided to hang on to a copy of this file in case it is needed for later reinstallations. The set-up process then proceeds, following standard lines. The process takes not much more than a minute in all, including the time taken to download the initial file, and completes with a reboot required. On restarting the machine for the first time after the install, a noticeable pause was observed before the system came fully to life – perhaps 30 seconds longer than the normal start-up time – but this did not happen on subsequent restarts. Updates were very speedy though, taking no more than 20 seconds to complete the full process even when using a fairly old copy of the main installer.

The interface is clean and professional-looking, providing a little more than the basic set of controls. Logging is clearly displayed in the product GUI, but for handling large amounts of data is something of a nightmare; with no option to export to text, data has to be decrypted from a bizarre and esoteric database format, which despite repeated pleas to the developers we are still forced to rip apart as best we can.

Operation of the product itself is less troublesome though, and speed tests proceeded without problems. Scan times were not bad, overheads rather heavy, and although RAM use was low, CPU use was pretty high and our set of tasks took a very long time indeed to get through. Detection, as

far as we could judge from our rather brutal unpicking of log data, was rather uninspiring in the Response sets, with no RAP scores for comparison, and although the WildList sets were properly dealt with on access, the on-demand jobs required data from the logs which appeared to show a number of items not covered, despite careful picking through them for any trace of the missing data.

We are thus forced to deny *Iolo* a VB100 award once again, the vendor's record now showing four fails from four attempts in the last six tests; two passes and five fails in the last two years, although it seems probable that some of these are entirely due to the lack of usable log data to process; we repeat our request to the developers to provide some more reliable way of accessing the information their product stores. Stability was good throughout though, meriting a 'solid' rating.

K7 Total Security

Main version: 12.1.0119
Update versions: 9.144.7068, 12.1.0124/9.145.7253, 9.145.7298, 9.145.7329

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Coming into this test we were told that *K7*'s product had had a bit of a refresh. The 84MB installer ran very simply with just a single click required, and completed very speedily, which was all the more impressive given that initial updates were included in the process. No reboot was required to get at the new GUI, which certainly looks very different. Gone is the wordy layout and gaudy colour scheme of the previous incarnation, replaced with a much simpler and clearer layout, featuring a brushed-metal-effect colour scheme and military fonts, giving it a robust and solid feel. Configuration is fairly thorough and easy to navigate, and logging is clear and reliable.

Scanning speeds were reasonable if not super fast, file access lags fairly light, with average resource use and a good time in our set of tasks. Detection was pretty good too – perhaps not quite up with the very best this month, but not far behind. The core sets presented no difficulties,
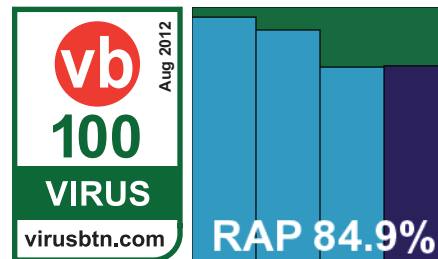
Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities time increase	Performance measures contd.	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities time increase
Agnitum Outpost	15.38%	15.25%	52.40%	14.44%	GFI VIPRE	5.30%	6.06%	18.54%	9.76%
AhnLab V3	3.95%	3.84%	9.29%	20.99%	Hauri ViRobot I.S.	5.94%	5.12%	162.35%	28.98%
Auslogics Antivirus	8.59%	8.60%	24.52%	20.45%	Ikarus virus.utilities	8.03%	7.50%	72.26%	13.73%
Avast Free Antivirus	8.14%	8.41%	33.88%	29.80%	Iolo System Shield	6.38%	4.91%	86.22%	163.25%
AVG I.S.	8.77%	11.69%	49.90%	31.23%	K7 Total Security	10.90%	10.31%	20.66%	15.77%
Avira Free Antivirus	5.04%	4.73%	31.13%	32.06%	Kaspersky E.S.	8.23%	9.16%	92.22%	48.03%
Avira Pro Security	4.59%	5.02%	32.56%	33.06%	Kaspersky I.S.	7.22%	8.30%	47.84%	17.72%
Bitdefender AV Plus	5.30%	4.91%	0.32%	23.68%	Lavasoft Ad-Aware	7.71%	6.87%	23.03%	4.86%
BullGuard	7.56%	5.71%	68.95%	23.13%	McAfee VirusScan	6.92%	5.47%	23.36%	18.54%
Central Command	7.85%	7.90%	15.94%	19.40%	Microsoft S.E.	5.68%	5.72%	26.57%	5.01%
CMC I.S.	11.04%	9.34%	8.95%	108.61%	Norman S.S.	8.26%	7.39%	38.62%	11.45%
Commtouch Command	4.66%	3.36%	84.27%	161.84%	Optenet S.S.	9.80%	9.97%	32.39%	60.65%
Comodo Antivirus	5.07%	4.88%	21.68%	13.18%	Panda Cloud AV	10.72%	10.61%	27.18%	54.14%
Coranti 2012	15.95%	19.29%	31.07%	13.75%	PC Tools I.S.	10.77%	11.80%	16.79%	62.41%
Defenx S.S.	11.39%	11.29%	63.29%	64.00%	PC Tools S.D	5.85%	5.83%	52.42%	29.04%
eEye Blink Pro	6.50%	5.07%	52.40%	18.87%	Qihoo 360 Antivirus	5.52%	6.60%	1.46%	9.24%
Emsisoft Anti-Malware	5.26%	7.47%	12.65%	29.01%	Quick Heal TS	22.30%	21.84%	24.33%	17.58%
eScan I.S.S.	13.61%	14.89%	154.67%	24.43%	Roboscan Enterprise	4.79%	6.16%	28.53%	19.55%
ESET NOD32	8.33%	8.50%	1.56%	43.59%	Sophos E.S.C.	9.59%	9.47%	26.85%	17.93%
ESTsoft ALYac	3.94%	4.97%	23.18%	5.78%	Tencent PC Manager	11.29%	13.36%	25.20%	10.61%
Filseclab Twister AV	10.15%	10.61%	21.47%	17.93%	Total Defense I.S.S.	12.61%	12.32%	31.21%	15.65%
Fortinet FortiClient	11.56%	9.31%	4.54%	90.61%	Total Defense T.D. r12	19.72%	19.75%	42.01%	24.17%
Frisk F-PROT	7.03%	6.73%	43.34%	2.19%	TrustPort Antivirus	5.89%	5.89%	65.23%	0.91%
F-Secure C.S.	10.44%	10.13%	1.02%	36.83%	VirusBuster Pro	10.12%	10.29%	22.66%	16.28%
F-Secure I.S. 2012	10.85%	10.14%	9.50%	31.93%	ZeoBIT PCKeeper	10.93%	10.54%	17.20%	26.59%
G Data AntiVirus 2013	11.14%	8.36%	21.14%	175.16%					

Please refer to text for full product names.

comfortably earning the product a VB100 award and continuing a good run of success, which thanks to a sporadic pattern of entries means only three passes in the last six tests, from three attempts; five passes from five entries in the last two years. Stability was not a problem, earning a 'solid' rating.

Kaspersky Endpoint Security 8 for Windows

Main version: 8.1.0.831
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

A pair of products came in from *Kaspersky* as usual, with both enterprise and consumer product lines represented. First up is the business product, which was provided as a 318MB package with updates for the RAP tests rolled in. The set-up process runs through a number of steps but doesn't take too long, completing in not much more than a minute. The initial install did not require a reboot, but some later updates did. In some cases this was not made very clear at all, with a small message in the product's logging interface informing the user that the machine must be restarted for the product to function fully.
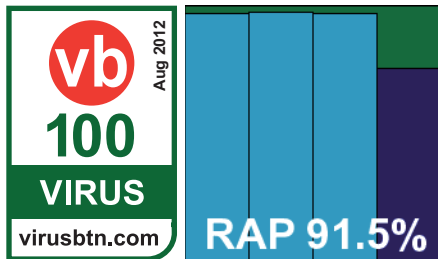
The GUI itself is sharp and stylish, a little quirky but reasonably simple to operate and providing an impeccable range of controls. Logging is also comprehensive and lucid with plenty of options to export to file. Scanning speeds were mostly a little slow to start with, but much faster in the warm runs. In the miscellaneous set however, we once again saw scans lasting an age, in some cases appearing to stop altogether. This was finally traced to a single rather large archive dropped as a temporary file by some installer, which was not being dealt with very well. On access it appears to have caused no problems though, with incredibly low overheads across the board. RAM use was average but CPU use a little high, with a fairly notable impact on our set of tasks too.

Detection rates were very solid though, a little behind the leading pack in the proactive week of the RAP sets but pretty impressive everywhere else, and with no issues in the

core sets a VB100 award is well earned, putting *Kaspersky*'s business line on four passes and one fail in the last six tests; eight passes and three fails in the last two years with a single test skipped. With the only issue noted being the poor handling of a deeply nested archive, a 'stable' rating is earned.

Kaspersky Internet Security 2013

Main version: 13.0.0.3370
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The consumer offering from *Kaspersky* is a little glitzier than its business counterpart but is usually found to be fairly similar under the covers. This month it was provided as a set of install files plus update data, the whole thing totalling a whopping 764MB but including a lot of additional data for the updating of other products. Set-up was very simple with an express install method requiring only a couple of clicks, completing in around two minutes with no reboot needed; updates were a little speedier here, averaging around four minutes.
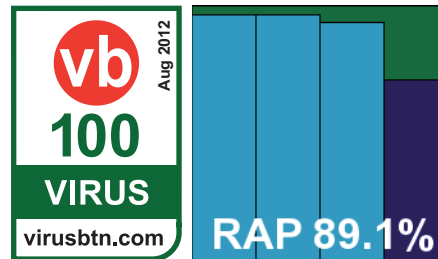
The interface is shiny and sparkly but does not skimp on the fine-tuning controls, providing ample configuration. Logging is again comprehensive, clear and easy to export. Scanning speeds were rather sluggish, with only some runs showing improvements in the warm scans, and again the set of 'other file types' took a long time to get through. On-access speed tests hit a problem at some point, the job freezing up part way through and still not having completed after being left alone for a full weekend. It seemed fine when we re-ran it though, although overheads were rather higher than expected. RAM use was a low average, CPU a little high, and our set of tasks got through in good order.

Detection was again very solid, with only the proactive week of the RAP sets lagging behind the best. The core sets were well handled and a VB100 award is earned, our history for this product line showing four passes and a single fail in the last six tests; eight passes and two fails in the last two years. With a couple of minor snags encountered, our rating is 'stable'.

Performance measures

Please refer to text for full product names.

Legend:
- Idle RAM usage increase
- Busy RAM usage increase
- Busy CPU usage increase
- Standard file activities - time increase

Products (vertical axis, top to bottom):
F-Secure IS 2012, F-Secure Client Security, Frisk F-PROT, Fortinet FortiClient, Filseclab Twister, ESTsoft ALYac, ESET NOD32, eScan ISS, Emsisoft Anti-Malware, eEye Blink, Defenx Security Suite 2012, Coranti 2012, Comodo AV, Commtouch Command, CMC Internet Security, Central Command Vexira, BullGuard, Bitdefender 2013, Avira Pro, Avira Free, AVG IS, Avast Free AV, Auslogics AV, AhnLab V3, Arphium Outpost

Horizontal axis: 0%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, 100%

Performance measures contd.

Please refer to text for full product names.

Legend:
- Idle RAM usage increase
- Busy RAM usage increase
- Busy CPU usage increase
- Standard file activities - time increase

Products (axis labels):
G Data AV 2013, GFI VIPRE 2012, Hauri ViRobot, Ikarus virus.utilities, Iolo System Shield, K7 TotalSecurity, Kaspersky Endpoint Security, Kaspersky IS 2013, Lavasoft Ad-Aware Free, McAfee VirusScan, Microsoft Security Essentials, Norman Security Suite, Optenet Security Suite, Panda Cloud AV PRO, PC Tools Internet Security, PC Tools Spyware Doctor, Qihoo 360 Antivirus, Total Security, Sophos Endpoint, Tencent PC Manager, Total Defense LS.S, Total Defense r12, Trustport Antivirus 2012, Trustport Antivirus 2013, Virusbuster Professional, Zeobit PCKeeper

Lavasoft Ad-Aware Free Antivirus +

Main version: 10.1.211.3382

Update versions: 12086, 12272, 10.2.21.3698

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	99.90%	**ItW Extd (o/a)**	99.90%
False positives			0

Lavasoft's *Ad-Aware* made a handful of appearances in our comparatives in 2010 with somewhat mixed success, stability issues hampering each attempt at testing. Since then a different product line, the '*Total Security*' brand based on a solution from *G Data*, has taken part in a few tests and fared rather better, so it was interesting if not entirely encouraging to see the mainline product back on the test bench.
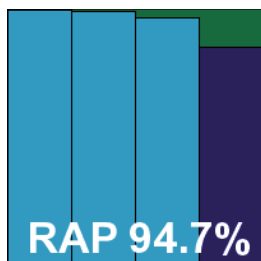
RAP 94.7%

The initial install package provided was very compact at just 6MB; installation displayed a large and brightly coloured set of dialogs, including one offering a browser add-on and a change of default search provider to the *blekko* service. The set-up proceeds through a rapid download of main components and a minute or two of installing work, some additional updating with a reboot to complete. On most runs this process was enlivened by a number of error messages, of the kind in which coded addresses for memory locations are described as inappropriately referencing other locations – which is of little use to the general user. More than 30 such messages were displayed during the downloading stages on almost all installs, with a handful more shortly afterwards on some (which seemed to be caused by opening *Paint* to record screenshots of the earlier alerts) – but out of kindness we have classed this as a single bug for the purposes of our rating system.

With speedy clicking through the error messages, things did proceed reasonably well, and most installs seemed to work OK despite the warnings. The interface has been completely revamped since we last saw it, and looks much more sturdy and serious, providing a reasonable level of control. Logging uses the same XML format as *GFI*'s *VIPRE*, the core engine of which is included here, and is thus rather unfriendly for reading purposes as well as inefficient and prone to flakiness. We saw several scan jobs falling over with no data salvageable, the RAP test requiring six installations and more than four full days to get a full set of figures. Other tests were also hit by other problems, with one scan job simply freezing up and making no progress over an entire weekend, while all attempts at on-access tests

over the fairly small WildList sets left the product interface locked up and unresponsive, with even rebooting failing to bring it around in some cases – instead, a very small and empty window was displayed when trying to open the product interface. On these occasions the installation was abandoned as irreparable, the system wiped and work restarted.

We did eventually get all we needed though, after relegating the product to our pile of lowest-priority 'joke' products, to be worked on as best we could but not worth devoting time to if it could be better spent ensuring fully functioning products were tested on schedule. Scanning speeds were slow, lag times not too bad on access – which was probably helped by the product not fully checking some items immediately, but allowing access initially and marking them as bad retrospectively. Resource uses were low and our set of tasks got through in good time, while detection rates were very good.

The clean sets were managed decently, but in the WildList sets once again after two perfect scores a handful of items were missed on the final run, thanks to hitting the same window of absence which affected the *GFI* product. So no VB100 award can be granted to *Lavasoft* this month. The product now has two fails from two attempts in the last two years. Stability was hit by a wide range of mostly quite serious problems, and is rated 'flaky'.

McAfee VirusScan Enterprise 8.8

Main version: 5400.1158

Update versions: 6747.0000, 6767.0000, 6773.0000, 6777.0000

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

McAfee's products have been taking part in around half of our comparatives for the last couple of years, but have had no problems for a

vb 100 Aug 2012
VIRUS
virusbtn.com

RAP 81.1%
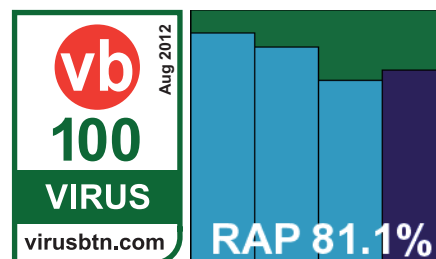
while and the vendor's corporate product at least is always a pleasure to test. The latest version was provided as a 38MB main installer with updates for the RAP tests measuring around 100MB; set-up is fairly simple and speedy with no surprises, and at the end the user is advised that a reboot is

required for some features of the product, but basic malware protection at least is in place from the off. Updates were also speedy and stable.

The GUI is very plain and simple but provides a comprehensive set of controls and is easy to navigate and operate, with no stability issues even under heavy pressure. Logging is similarly complete and reliable, with easy-to-read text format available for several separate areas. Scanning speeds were nice and fast, overheads reasonable with default settings, speeding up a lot in the warm runs, a little higher with settings turned right up. Resource use was low and our set of tasks completed in average time.

Detection rates were decent if not spectacular in the RAP sets, with a fairly steep decline through the weeks, but the Response sets were much better thanks to cloud look-ups. The core sets were ably dealt with and a VB100 award is earned without fuss, putting *McAfee* on three passes from three entries in the last six tests; five passes and a single fail from six attempts in the last two years. A thoroughly solid and businesslike performance earns a 'solid' stability rating.

Microsoft Security Essentials

Main version: 4.0.1526.0
Update versions: 1.1.8502.0/1.129.24.0, 1.1.8502.0/1.129.1379.0, 1.1.8601.0/1.131.70.0, 1.1.8601.0/1.131.485.0

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Microsoft's free-for-personal-use solution also appears only in alternate tests, in this case alternating with the business-focused *Forefront*. The *Essentials* install package is very compact at just 10MB, with updates not too large either at 60MB for the offline install bundle. Set-up is pretty fast and simple, with the only feature of note being an 'optimization' stage which seems mainly to involve checking that things such as the *Windows* firewall and update systems are switched on and functioning properly. Taking less than half a minute to complete, updates are also speedy, putting the total install time at little over a minute with no reboots required.
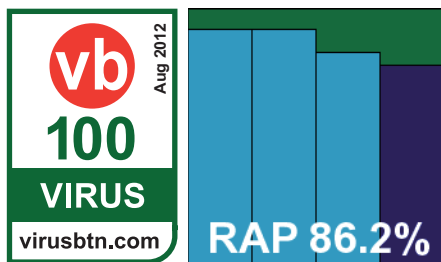
The interface looks fairly pleasant, providing only limited controls and seeming perhaps a shade wordy in places, but it is mostly fairly simple to navigate and operate. Logging is a little spread around and hard to find, but once the system is figured out it proves complete, clear and reliable. Scanning speeds were decent, overheads a little higher than average on first encountering items but much quicker in the warm runs. Resource use was low and our activities measure was also very zippy.

Detection rates were decent, with a consistent level in the earlier weeks of the RAP sets and not too much of a decline in the later weeks. The core sets presented no issues and a VB100 award is comfortably earned, putting the product on three passes from three attempts in the last six tests; five from five in the last two years. No stability problems were encountered at all, earning the product a 'solid' rating.

Norman Security Suite

Main version: 9.00
Update versions: 6.08.06

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Norman's participation in our comparatives is very regular indeed, with tests very rarely missed. The current product came
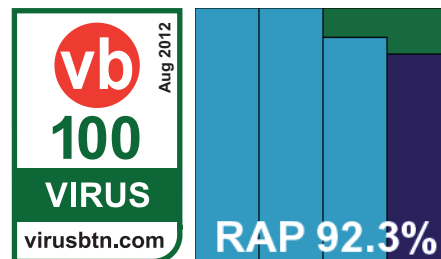
as a 184MB installer with latest updates rolled in, and ran through the standard set of steps, the dialogs completing fairly quickly while some more time was required for background tasks to finish before the product was fully in place and a reboot requested. Updates were a little uneven, with some taking only five minutes, others more than 10. The interface is a little fiddly and prone to losing settings, thanks to its lack of any warnings when navigating away from a page without having spotted the 'save changes' button. Logging is clear, reliable and usable though.

Scanning speeds were slow and overheads fairly high, but resource use was reasonable and our set of tasks didn't take too long to complete. Detection rates were very good indeed, continuing a recent run of improvements, and the core sets were handled properly (somewhat to our surprise, considering a problem noted in another implementation

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	OD	X	√	√	√	√	X	√	5	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
AhnLab V3	OD	X	X	X	X	√	√	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Auslogics Antivirus	OD	√	√	7	7	√	√	√	7	√	√	√
	OA	X/2	X/2	X/1	X/1	2	X/2	X/2	X/1	1/2	1/2	√
Avast Free Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
AVG Internet Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira Free Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avira Professional Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Bitdefender Antivirus Plus 2012	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
BullGuard	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	2	2	1	1	2	2	2	1	2	2	√
Central Command Vexira	OD	X	√	√	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
CMC Internet Security	OD	X	X	X	X	X	X	X	X	X	X	X
	OA	X	X	X	X	X	X	X	X	X	X	X
Commtouch Command Anti-Malware	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2	2	2	2	2	√	2	1	2	2	√
Comodo Antivirus	OD	X	5	5	5	5	5	5	5	2	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Coranti 2012	OD	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
	OA	X	X	X	X	X/√	X	X	X/1	1	X	X/√
Defenx Security Suite 2012	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
eEye Blink Professional	OD	X	1	1	1	1	1	1	8	2	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Emsisoft Anti-Malware	OD	2	2	X	X	2	2	2	3	2	2	√
	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

* 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*
eScan Internet Security Suite	OD	X	X	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ESET NOD32 Antivirus 5	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ESTsoft ALYac Enterprise	OD	X	X	8	8	√	√	X	8	√	1	√
	OA	X	X	8	8	X	X	X	X	X	X	√
Filseclab Twister Antivirus V7	OD	5	3	3	3	4	1	4	X	5	X	√
	OA	X	X	X	X	X	X	1	X	2	X	X
Fortinet FortiClient	OD	1	√	√	√	√	√	√	√	√	√	√
	OA	1	√	√	√	√	√	√	√	√	√	√
Frisk F-PROT Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	2	2	X	X	X	X	2	2	√
F-Secure Client Security	OD	X/√	√	√	√	√	√	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure Internet Security	OD	X/√	√	√	√	√	√	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X
G Data AntiVirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
GFI VIPRE Antivirus 2012	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Hauri ViRobot Internet Security	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Ikarus virus.utilities	OD	7	7	7	7	7	7	7	3	7	7	√
	OA	7	7	7	7	7	7	7	3	7	7	√
Iolo System Shield	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2	2	2	2	2	√	2	1	2	2	√
K7 Total Security	OD	√	√	√	√	√	√	√	X	√	√	√
	OA	X	X	X	1	1	X	X	X	1	1	√
Kaspersky Endpoint Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kaspersky Internet Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Lavasoft Ad-Aware Free AV +	OD	X	X	√	√	√	X	√	X	√	X	√
	OA	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

* 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*
McAfee VirusScan Enterprise	OD	2	√	√	√	√	√	√	√	√	X	√
	OA	2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X	√
Microsoft Security Essentials	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√
Norman Security Suite	OD	X	√	√	1	√	√	√	8	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Optenet Security Suite	OD	X	X	1	1	X	X	X	X	X	X	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Panda Cloud Antivirus PRO	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	2	X	X
PC Tools Internet Security	OD	1	√	6	√	√	√	√	5	√	√	√
	OA	X	X	2	2	X	X	X	X	X	X	X
PC Tools Spyware Doctor	OD	1	√	6	√	√	√	√	5	√	√	√
	OA	X	X	2	2	X	X	X	X	X	X	X
Qihoo 360 Antivirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Quick Heal Total Security	OD	X/1	2/5	1/2	1/2	2/5	X	2/5	2/11	2/5	X	√
	OA	1	X	2	2	1	X	X	X	1	X	√
Roboscan Enterprise Solution	OD	X	X	8	8	√	√	X	8	√	1	√
	OA	X	X	8	8	X	X	X	X	X	X	√
Sophos Endpoint Security and Control	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Tencent PC Manager	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Total Defense Inc. Internet Security Suite	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Total Defense Inc. Total Defense r12	OD	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
TrustPort Antivirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	√	X	X	X	1	1	√
VirusBuster Professional	OD	2	√	X	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
ZeoBIT PCKeeper	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	1	1	1	1	1	1	1	X	1	1	√

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

* Detection of EICAR test file with randomly chosen file extension

Please refer to text for full product names.

of the same engine elsewhere in this test). A VB100 is well deserved then, putting *Norman* on a perfect six out of six in the last year; 11 passes and a single fail in the last two years. A single instance of the GUI freezing up under pressure means a perfectly respectable 'stable' rating.

Optenet Security Suite

Main version: 10.09.70

Update versions: 3325

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	99.90%	**ItW Extd (o/a)**	99.90%
False positives			0

Headquartered in Spain and with much of its business done in South America, *Optenet* has appeared in a handful of comparatives already with its suite solution incorporating the *Kaspersky* engine. The installer submitted was a 158MB executable with updates rolled in for the RAP tests. Set-up is fairly straightforward, although rather unusually it does insist on setting up a password to access the control systems. A reboot is required to complete, and updates usually start automatically on restart; these ran through fairly quickly on some occasions, but on others it took much longer, with no dialog to follow and only a message displayed on hovering over the product's system tray icon showing that it was still under way. On some occasions a second reboot was needed on completion of this lengthy process, and on a few of these occasions updating restarted after the reboot.

RAP 90.2%
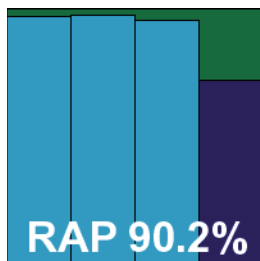
The product interface is a little unusual, with some oddities of phrasing making it harder to navigate than most, but with a little familiarization it soon becomes straightforward to find most functions, with configuration provided to a level a little above the basics. Logging is decent and readable.

Scanning speeds were fairly decent, overheads a little heavy and our set of tasks quite slow. Detection rates were solid in the RAP tests, with Response test scores certainly decent but perhaps just a little lower than we might have expected. The clean sets were well dealt with, and in the WildList sets coverage was almost perfect, but rather surprisingly a couple of items in the Extended list were missed. We looked into the logs from other products based on the same engine which didn't have this problem, and spotted that these two items were flagged as 'potentially dangerous' detections emanating from a cloud look-up system – which

presumably the *Optenet* product does not make use of. So, *Optenet* is denied certification this month by a whisker, having put in a generally decent showing. The vendor now has one pass and one fail in the last six tests; two passes and one fail in the last two years. With the interface locking up occasionally after large jobs, and the updater a little odd at times too, a 'stable' rating is earned.

Panda Cloud Antivirus PRO

Main version: 1.5.2

Update versions: 2.0.0

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

We arrive at something of a big moment here, as *Panda* makes its first appearance in our tests since 2002. Having been one of the first to leverage cloud technology, the vendor's products did not fit well with the *VB* testing system until the recent overhaul of our methodology, and we are pleased to see them returning to the test bench. The product submitted was the 'Pro' version of *Panda*'s cloud-based solution, but having looked at other variants including free editions, the main protective features seem comparable in most of them. The installer downloaded from the company's website was a tiny 600KB, fetching the rest of the product from the web at install time. This featured the usual welcome and EULA screens, selection of language and install locations, plus the offer of a security browser toolbar and setting the default search provider to *Google*, before completing almost instantly.

vb 100 VIRUS
Aug 2012
virusbtn.com

The interface is quite attractive, decorated in moody black and dark greys, with splashes of colour to highlight the various features and a *Facebook* 'like' button in one corner of the main screen. Configuration is provided in reasonable depth and is simple to navigate; logging was switched to 'extended' mode to ensure complete data availability, and this certainly made for some lengthy logs, with several hundred MBs of data to peruse by the end of testing. Somewhat unusually, this did not include information on what things were classed as in any more depth than 'malware' or 'clean'. This was enough for our needs, although it might have helped in the clean sets where initial processing brought up what seemed to be a false positive in a component of *IBM*'s *Lotus Notes*. Closer analysis by the eagle-eyed experts at *Panda* revealed the EICAR test string buried in the file for some reason, so the alert was treated as accurate, but had the lengthy logging included IDs for

Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive Average	Proactive Week +1	Overall Average
		Week -3	Week -2	Week -1			
Agnitum Outpost		85.04%	80.95%	70.95%	78.98%	61.71%	74.66%
AhnLab V3	VIRUS 100	85.32%	83.61%	77.03%	81.98%	79.26%	81.30%
Auslogics Antivirus‡	VIRUS 100	N/T	N/T	N/T	N/T	N/T	N/T
Avast Free Antivirus	VIRUS 100	98.56%	98.65%	95.28%	97.50%	73.18%	91.42%
AVG Internet Security	VIRUS 100	98.65%	97.55%	92.82%	96.34%	79.74%	92.19%
Avira Free Antivirus	VIRUS 100	99.16%	99.09%	94.30%	97.51%	89.52%	95.52%
Avira Professional Security	VIRUS 100	99.16%	99.09%	94.30%	97.51%	89.52%	95.52%
Bitdefender Antivirus Plus 2012	VIRUS 100	97.28%	98.19%	97.32%	97.60%	89.61%	95.60%
BullGuard	VIRUS 100	97.28%	98.19%	97.30%	97.59%	89.61%	95.59%
Central Command Vexira		84.98%	80.64%	70.40%	78.67%	61.27%	74.32%
CMC Internet Security		66.66%	61.76%	60.63%	63.02%	57.16%	61.55%
Commtouch Command Anti-Malware	VIRUS 100	64.15%	71.76%	66.81%	67.57%	70.76%	68.37%
Comodo Antivirus‡		N/T	N/T	N/T	N/T	N/T	N/T
Coranti 2012	VIRUS 100	98.05%	98.81%	98.29%	98.38%	92.42%	96.89%
Defenx Security Suite 2012		84.93%	80.88%	70.90%	78.90%	61.57%	74.57%
eEye Blink Professional		99.59%	99.60%	91.67%	96.96%	82.55%	93.35%
Emsisoft Anti-Malware		99.50%	99.47%	95.37%	98.12%	87.06%	95.35%
eScan Internet Security Suite	VIRUS 100	97.26%	98.19%	97.28%	97.58%	89.63%	95.59%
ESET NOD32 Antivirus 5	VIRUS 100	94.81%	86.09%	91.26%	90.72%	70.43%	85.65%
ESTsoft ALYac Enterprise		94.94%	95.97%	93.21%	94.71%	86.91%	92.76%
Filseclab Twister Antivirus V7		91.54%	92.13%	87.78%	90.49%	81.91%	88.34%
Fortinet FortiClient	VIRUS 100	98.98%	99.05%	96.83%	98.29%	89.28%	96.04%
Frisk F-PROT Antivirus	VIRUS 100	60.12%	68.31%	62.77%	63.73%	68.09%	64.82%
F-Secure Client Security	VIRUS 100	97.28%	98.21%	95.45%	96.98%	74.75%	91.42%
F-Secure Internet Security 2012†	VIRUS 100	N/T	N/T	N/T	N/T	N/T	N/T
G Data AntiVirus 2013	VIRUS 100	99.82%	99.82%	97.79%	99.14%	90.84%	97.07%

N/T - Not tested.

* Product requires live connection for full functionality.

† Product omitted at submitter's request.

‡ Product omitted due to technical issues.

Please refer to text for full product names.

Reactive And Proactive (RAP) tests contd.	VB100	Reactive			Reactive Average	Proactive Week +1	Overall Average
		Week -3	Week -2	Week -1			
GFI VIPRE Antivirus 2012		99.04%	98.82%	95.56%	97.81%	84.29%	94.43%
Hauri ViRobot Internet Security 2011	VIRUS 100	97.24%	98.18%	97.27%	97.57%	89.58%	95.57%
Ikarus virus.utilities		99.85%	99.64%	95.38%	98.29%	87.14%	95.50%
Iolo System Shield†		N/T	N/T	N/T	N/T	N/T	N/T
K7 Total Security	VIRUS 100	95.75%	90.84%	76.07%	87.55%	76.98%	84.91%
Kaspersky Endpoint Security	VIRUS 100	96.98%	97.28%	96.57%	96.94%	75.01%	91.46%
Kaspersky Internet Security 2013	VIRUS 100	96.24%	96.31%	93.37%	95.31%	70.65%	89.14%
Lavasoft Ad-Aware Free Antivirus +		99.06%	98.82%	96.26%	98.05%	84.68%	94.70%
McAfee VirusScan Enterprise	VIRUS 100	90.77%	85.22%	72.04%	82.68%	76.22%	81.06%
Microsoft Security Essentials	VIRUS 100	91.99%	91.98%	82.85%	88.94%	77.91%	86.18%
Norman Security Suite	VIRUS 100	99.58%	99.59%	88.31%	95.83%	81.82%	92.32%
Optenet Security Suite		96.78%	97.12%	95.11%	96.34%	71.81%	90.21%
Panda Cloud Antivirus PRO*	VIRUS 100	N/T	N/T	N/T	N/T	N/T	N/T
PC Tools Internet Security	VIRUS 100	88.01%	89.06%	78.41%	85.16%	64.25%	79.93%
PC Tools Spyware Doctor	VIRUS 100	88.01%	89.06%	78.41%	85.16%	64.25%	79.93%
Qihoo 360 Antivirus	VIRUS 100	96.26%	97.34%	93.79%	95.80%	86.58%	93.49%
Quick Heal Total Security 2012		89.84%	87.97%	76.04%	84.62%	75.23%	82.27%
Roboscan Enterprise Solution		94.97%	95.98%	93.27%	94.74%	86.94%	92.79%
Sophos Endpoint Security and Control	VIRUS 100	84.76%	85.07%	80.27%	83.37%	74.90%	81.25%
Tencent PC Manager	VIRUS 100	99.29%	99.13%	95.85%	98.09%	89.93%	96.05%
Total Defense Inc. Internet Security Suite†	VIRUS 100	N/T	N/T	N/T	N/T	N/T	N/T
Total Defense Inc. Total Defense r12	VIRUS 100	60.57%	60.11%	54.30%	58.33%	43.67%	54.66%
TrustPort Antivirus 2013	VIRUS 100	97.24%	98.17%	97.06%	97.49%	89.48%	95.49%
VirusBuster Professional		84.99%	80.64%	70.47%	78.70%	61.27%	74.34%
ZeoBIT PCKeeper	VIRUS 100	99.34%	99.16%	98.00%	98.83%	92.35%	97.21%

N/T - Not tested.
* Product requires live connection for full functionality.
† Product omitted at submitter's request.
‡ Product omitted due to technical issues.
Please refer to text for full product names.

detection, as most vendors seem to do, the problem would have been much simpler to resolve.

Speed measures were pretty decent – a little slower over archives thanks to very thorough defaults; on-access measures look very light, but on-read scanning seems to be limited to certain types of files, and all on-access detection measures were taken on-write. Resource use was perhaps a shade above average, and our set of activities took a little longer to complete than many this month but slowdown was not too intrusive.

Operating entirely from the cloud, it was of course impossible to include the product in the RAP test, but Response scores were excellent, with an average among the very highest this month. With the single scare in the clean sets quickly eradicated, the WildList sets were well covered too, earning *Panda* a VB100 award on its first visit back to the tests after a decade away. A single issue was noted, when a scan of part of the clean sets froze up requiring a reboot to complete, but this did not recur on re-running the job; a 'stable' rating is thus awarded.

PC Tools Internet Security

Main version: 9.0.2298
Update versions: 369788/6.19950, 372237/6.20180, 373320/6.20200

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Back to a somewhat more regular participant in our comparatives, *PC Tools* tends to enter only on desktop platforms,

RAP 79.9%
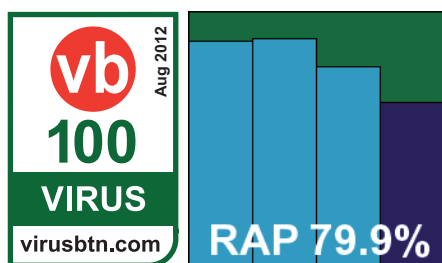
but makes up for it by invariably submitting a pair of products. The suite solution comes first, with a 271MB installer containing all required data. Installation was fairly standard and reasonably brief, taking around a minute for the main install and a couple more for some 'initialization' steps. Updates were also fairly fast, averaging just over three minutes. An initial scan would then be launched, which would usually manage to warn about a few 'tracking cookies' before we had time to cancel it.

On some, but not most installs, things would then slow down considerably. Running our on-access job over the

WildList sets (usually the first thing performed on each of the main runs) would take around 8–10 minutes in general, where the fastest products this month needed perhaps four minutes. On at least two installs though, the job took over nine hours, spending quite some time on each sample before deciding to block it, and at some point giving up, with over half the set ignored, showing that protection had ceased to function. Reinstalling on a fresh machine the following day proved much more successful, with the same task running at good speed and with no sign of misses.

Once we had figured out this pattern and knew what to look out for, it was easy enough simply to give up on the duff installations and wipe systems for a fresh start, but for normal users it might be less easy to go through the process of uninstallation cleanly. Eventually we managed to gather all the data required, which showed some slowish scan times speeding up a lot in the warm runs, RAM use a little high but CPU use not bad at all, and a fairly heavy impact on our set of tasks.

Detection rates were once again tricky to work out, as logging is bizarre in the extreme: data is written to XML-format logs, but these are removed after some period – presumably sent back to base for some sort of feedback system, but either way no longer available to the actual user. A tool was provided to circumvent this, and also to get around the rather complex system of having items flagged as suspect but then much later marked as 'exonerated' by cloud look-ups. We were able to piece together what we needed, and saw RAP scores starting fairly decently but declining fairly sharply in the later weeks, Response scores were considerably better thanks to the cloud system but again showed a steady downward trend through the days, until a surprise resurgence in the most recent day.

The core sets were handled well with no issues, and a VB100 award is earned, making three passes from three attempts in the last six tests; five passes and a single fail in the last two years. There were some pretty serious issues with several of the installs though, making for a stability score at the upper end of the 'fair' range.
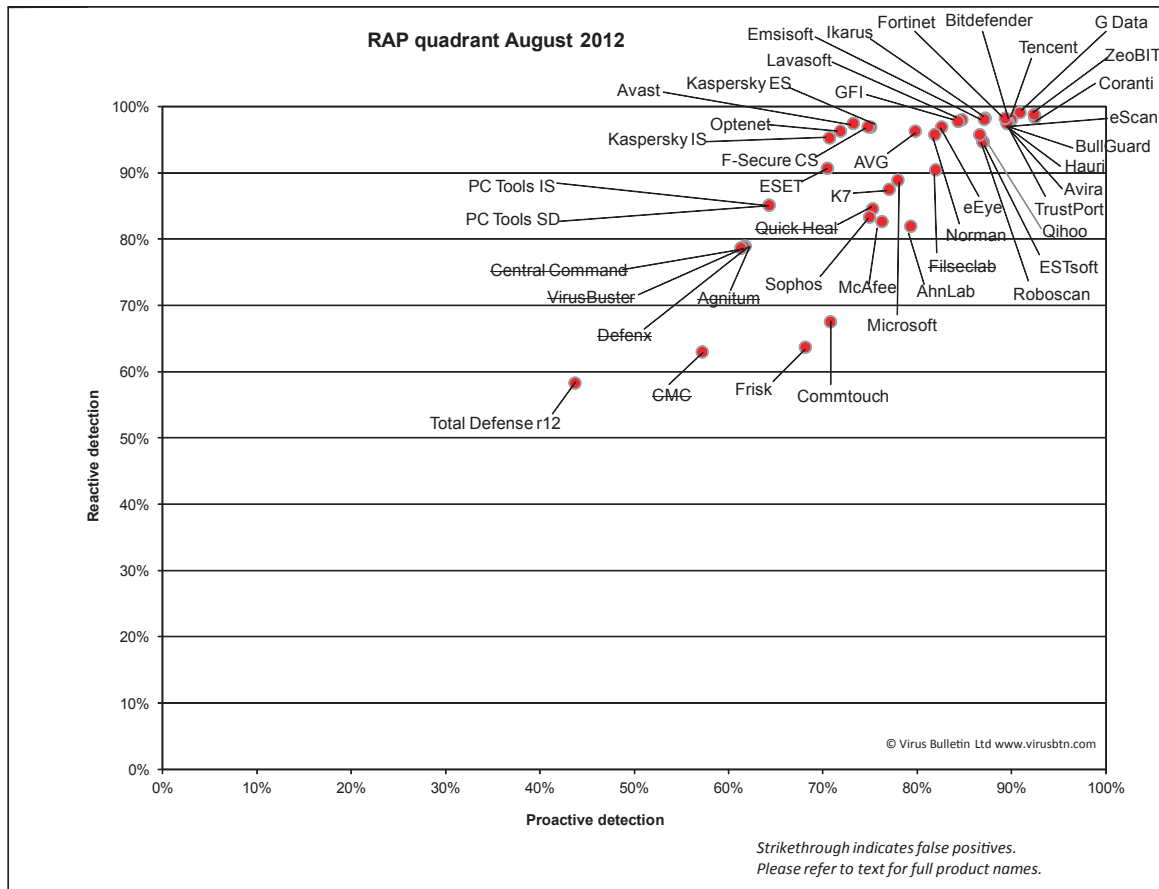
PC Tools Spyware Doctor

Main version: 9.0.0.2298
Update versions: 369788/6.19950, 372237/6.20180, 373320/6.20200

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The second offering from *PC Tools* this month is its renowned *Spyware Doctor*, which we have generally found to be extremely similar to the suite line, minus the firewall

RAP quadrant August 2012

Strikethrough indicates false positives.
Please refer to text for full product names.

and perhaps a few other components. We hoped this month to see some bigger differences though, given the issues we had already experienced.
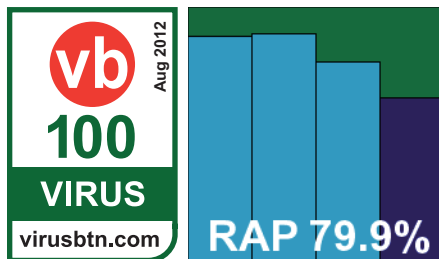
The installer this time was 271MB, and again the set-up was lacking in surprises and reasonably fast, with updates similarly quick and a total install time of around five minutes. The interface is similarly colourful, glossy and short on controls, with logging restricted once again to data gathered for the developers rather than the user. Scanning speeds were similar initially, putting them on the slow side, with a considerably more noticeable improvement in the warm runs this time, while overheads on access were a little lighter. RAM use was below average, CPU use well over, and our activities took a fair while to get through, but

considerably less than the suite product (presumably thanks to less inspection of networking activity and the superior caching).

Detection scores were very similar though – identical in most respects, with RAP scores exactly the same and Response scores varying only very slightly, thanks to being run at slightly different times. The core sets were properly dealt with, so *Spyware Doctor* also earns a VB100 award, its history matching the suite with three passes from three attempts in the last six tests; five passes and a single fail in the last two years. In the stability measures *Spyware Doctor* fared slightly better, with several installs again showing severe slowdowns in some tests, but we didn't see any instances of protection failing (perhaps more through luck than good design). *Spyware Doctor* therefore just scrapes a 'stable' rating.

Qihoo 360 Antivirus

Main version: 3.0.0.3051

Update versions: 2012-06-17, 2012-07-11, 2012-07-17, 2012-07-23

Qihoo 360 Antivirus contd.

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Returning to our *Bitdefender* theme, *Qihoo*'s *360* has been a fairly regular participant in our tests for a few years, with a rather uneven pattern of performances. The current product came as a 122MB installer, which ran with minimal interaction, completing in around a minute with no reboot required, and online updates added no more than two further minutes. The interface has seen a few minor improvements of late, adding a little more gloss while sticking to the same basic design, which is fairly clear and usable and provides a reasonable set of controls. A log viewer tool is provided, which seems to work well and allows easy exporting of data to text.
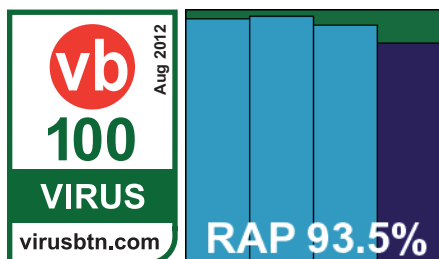
Scanning speeds were rather slow, and overheads perhaps a little high, but resource use was low – especially the CPU measure – and our set of tasks tripped through in short order. This may be a little misleading though, as on-read scanning seems not to be implemented and on-write scanning is rather bizarre. Clearly, the product does not perform proper pre-emptive scanning and instead checks things in a leisurely way, allowing them to be written and then presenting an alert dialog some time later, proudly (but rather misleadingly) informing the user that the activity has been blocked; fortunately it does seem to clamp down on things from there on, and actual execution is protected against properly.

Detection rates were very good – a fraction behind those of others using the same engine in the RAP sets thanks to some slightly older data included in the submission, but still highly competitive, and solid too in the Response sets. The WildList sets were handled well, albeit quite some time in arrears in the case of the on-access measures, and in the clean sets there were just a few warnings of possible archive bombs, so no showstoppers there either. A VB100 award is duly earned, marking *Qihoo*'s first pass from three attempts in the last six tests, although the two-year picture looks a little better with five passes and two fails. There were a few wobbly moments in the on-access tests when under pressure, but stability was generally good and a 'stable' rating is earned.

Quick Heal Total Security 2012

Main version: 13.00 (6.0.0.4)
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			1

Quick Heal is another very regular participant in the VB100 tests, with a long and respectable history, although a brief blip earlier this year saw its first absence from a test since 2006. The current product was provided as a fairly large 344MB package with all updates included. Set-up involves very few clicks, completing in under a minute with no reboot required. Updates run the download stage very quickly, but some extra time is taken afterwards as they are applied.
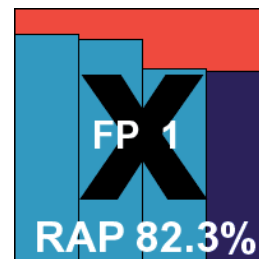
The interface is bright and cheerful, at times a little confusing in its operation but mostly fairly usable and with a good range of controls. Logging is clear and easy to use too.

Testing proceeded without problems, revealing some decent scanning speeds, a little lower over archives although both coverage of archive types and depth of scanning are rather limited. File access lags were fairly light though, while RAM use was fairly high, with reasonable CPU use and an average impact on our set of tasks.

Detection scores were not bad in the RAP sets, a little off the pace in the Response sets, but the WildList set was well covered. In the clean sets a single item, part of *Adobe Acrobat*, was labelled a trojan, denying *Quick Heal* a VB100 award this month and continuing its recent spell of bad luck. The vendor now has two passes and three fails from five entries in the last six tests; eight passes and three fails in the last two years. On the plus side, stability problems were completely absent, earning a rating of 'solid'.

Roboscan Enterprise Solution

Main version: 2.5.0.18
Update versions: 12.4.26.1/433901.2012061916/7.42659 /7309216.20120619, 12.4.26.1/436785.2012071117/7.43 864/7363079.20120710, 12.4.26.1/437480.2012071714/ 7.42897/7363560.20120715, 12.4.26.1/438143.2012072 313/7.42918/7360237.20120718

ItW Std	99.84%	**ItW Std (o/a)**	99.84%
ItW Extd	99.85%	**ItW Extd (o/a)**	99.80%
False positives			0

Roboscan is a pretty straightforward clone of *ESTsoft*'s *ALYac* product, already covered here, and it put in a pretty much identical showing. The 140MB installer ran along standard lines in decent time, needing no reboot, and updates were a little unpredictable in both length and chances of

RAP 92.8%

success. The GUI is clear and provides decent controls, with a log viewer which can take some time to deal with data, particularly when a lot has been happening. In the case of one of the RAP jobs, after the scan completed it was more than two hours until the logging system had finished processing its information, during which time the product was effectively unusable.
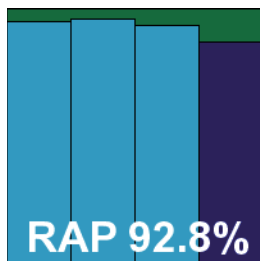
Nevertheless, there were few serious problems, and tests moved along nicely, showing fast scanning speeds, light overheads (particularly in the warm runs), and reasonably low resource use, with a good time for our set of tasks too. Detection was solid – a little lower than might be expected from the *Bitdefender* engine underlying things, but still pretty good. There were no issues in the clean sets, but once again a few items in the WildList sets were ignored for some reason, and a VB100 award cannot be granted to *Roboscan* this month. The vendor's brief history now shows one pass and one fail, both in the last few tests. A 'stable' rating is earned for this month's decent performance though.

Sophos Endpoint Security and Control

Main version: 10.0.5
Update versions: 3.31.20/4.78G, 10.0.6/3.33.2/4.79G

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another of our long-term regulars, *Sophos* hasn't had an absence from our comparatives since 2006. The current product was provided

RAP 81.3%

as a 98MB installer, with the offline update bundle only 4MB, making it one of the smaller products this month all in. Set-up has quite a few steps to click through compared to some, but there is little to tax the mind, completing in not
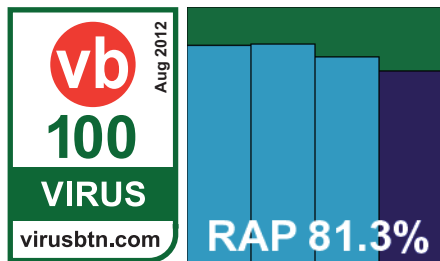
much over a minute, with later updates rarely adding more than another minute to the total install time.

The interface is angular and businesslike but not unfriendly, providing an impeccable range of fine-tuning with some seriously technical options available under the hood for those who want to fiddle with them (although this is not recommended without expert guidance). Operation was smooth and reliable, with clear logging in simple text format available throughout. Detection rates were decent if unspectacular in the RAP sets, considerably better in the Response sets thanks to additional cloud activity, and with no issues in the core sets a VB100 award is well deserved. No problems to report anywhere means a stability rating of 'solid'.
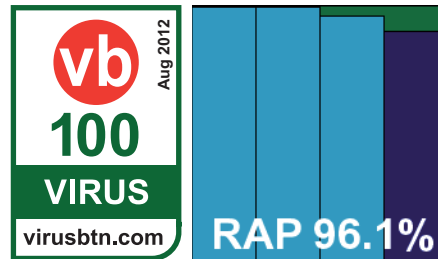
Tencent PC Manager

Main version: 6.6.2283.201
Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Another relative newcomer, *Tencent* has only a single, successful comparative under its belt, but seems set to do well thanks

RAP 96.1%

to the dependable *Avira* engine underlying the anti-malware component of the solution. Installation involves only three clicks, although exactly what we were clicking was not quite clear thanks to the absence of English translations of the product. Nevertheless, by following a detailed user guide provided by the developers, along with a little common sense and a feeling for where things tend to be in anti-malware products, operation was fairly straightforward. Little can be said about the interface other than that it is colourful, and seems to have a large number of controls, apparently offering a lot more besides the basics of malware detection.

Scanning speeds were impressively fast, with overheads very light too, a slight spike on the graph in the set of media and documents still not much higher than average. Resource use was a little above average, particularly RAM use, which is perhaps due to the wide range of features included here; our set of tasks got through in reasonable time.

Detection rates were excellent, with the RAP sets completely demolished and decent scores in the Response sets too, although here they were perhaps not quite as good as we might expect, hinting that updates are a little behind the very latest available. The core sets were well dealt with each time we checked though, and a second VB100 award is comfortably earned, while stability was 'solid'.

Total Defense Inc. Internet Security Suite

Main version: 8.0.0.87

Update versions: 5859.0.0.0, 5901.0.0.0, 5903.0.0.0

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

Total Defense sticks with its long tradition of entering two products for the desktop platforms. The consumer offering is apparently a little different this month as its developers requested it be left out of the RAP test since it relies on cloud connectivity. Otherwise things seemed much the same as usual though, with the 173MB installer large enough to suggest that at least some data is stored locally, and presenting just a large green 'Start' button before zipping through its business in a couple of minutes. It offers to install a *Yahoo!* toolbar at the end before requesting a reboot. On restart, some initial set-up including licensing and gathering some personal data is run through, but updates are over in a flash.

The interface is much as we have seen in previous tests, with the overall look fairly pretty but configuration a little confusing and limited to the basics. Scanning speeds were perhaps a little on the slow side first time around but powered through very quickly in the warm runs, while on-access overheads were a little higher than we're used to. Resource use and impact on our set of activities were reasonable though.

Detection rates were a little more problematic to measure, with any scan that covered more than a handful of detections hitting a snag at least once. The first scan of the Response sets simply vanished, quite without warning or explanation, while the second and third each got to the end and reported nothing found, despite having shown several thousand detections just moments earlier. Fortunately, re-running the same job seemed to iron out the problem, perhaps thanks to caching of results as in the speed tests, and things proceeded without too much bother.

The core sets were properly dealt with (and without scanning issues either), earning *Total Defense* a VB100

award and putting the vendor's consumer line on two passes and one fail in the last six tests; four passes and two fails in the last two years. With failed scans misinforming the user about the safeness of their system a few times, stability is rated as only 'fair'.
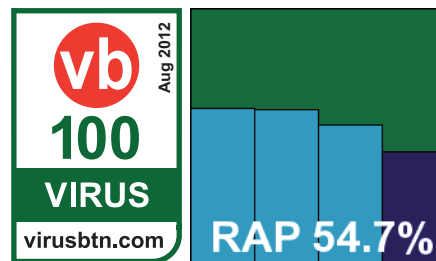
Total Defense Inc. Total Defense r12

Main version: 12.0.0.832

Update versions: 1.6.0.1844/5875.0.0.0, 5895.0.0.0, 5901.0.0.0, 5903.0.0.0

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The second product from *Total Defense*, the vendor's business offering, rarely misses a test of any kind, with this month's installation seeing a fresh download of the DVD image used for the set-up of submissions. The entire image is close to 4GB but includes a wide range of products alongside the basic client anti-malware looked at here. It was installed on the deadline day, going through a lengthy series of stages with lots of data needing to be filled in. As usual, licensing is a little confusing and at times frustrating, particularly when a long licence key is provided, but the dialog requesting it isn't smart enough to accept pasting the whole thing at once, instead requiring several copy-paste operations to fill in the code. We also observed that the address-gathering system still requires a US state and US-format zip code, whichever country is selected from the previous menu. We plumped for Arkansas this month. A reboot is required to complete the process; updates are very fast and efficient, taking less than 30 seconds even the first time after installation.

The GUI is unshowy but provides a decent level of control and mostly seems to work well; at one point it did seem to freeze up after some on-access tests, but a quick reboot straightened things out. Logging can be viewed inside the product in tiny chunks, but cannot be exported directly, although we would assume the management tools available alongside the client-side product would be better able to provide such assistance. The data is stored in standard SQL database format though, so was fairly simple to convert to plain text for our requirements.

Scanning speeds started out pretty fast and moved up several gears in the warm runs, while overheads were a little high, especially over the archive set with the settings turned up, as one might expect. Resource use was a little above average, as was impact on our set of tasks.

RAP scores were fairly mediocre, verging on the poor, as were figures for the Response sets, suggesting that the product could do with some of the cloud technology that boosted its consumer sibling's performance this month. The core sets were properly covered though, with no false alarms, and *Total Defense* earns a second VB100 this month. The vendor's business line now has four passes and one fail in the last six tests; eight passes and two fails in the last two years. With a few minor issues noted, a 'stable' rating is earned.

TrustPort Antivirus 2013

Main version: 13.0.1.5061

Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

TrustPort's latest version heralds the fast-approaching 2013, and sports a serious revamping compared to previous editions. The
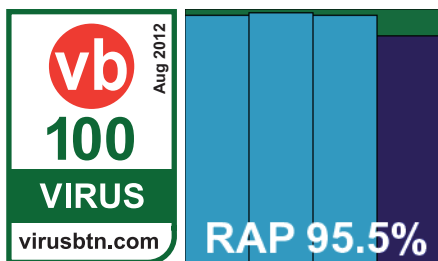
installer is not too large at 133MB including updates, and set-up is fairly simple and quick with no reboot required. Updates pull down upwards of 50MB of data but do so at a good pace, with the whole business taking not much more than three minutes. Observing the update process it was clear that only a single engine, identified as 'Xenon', was in place, so it would seem that *TrustPort* has abandoned its long habit of using a dual-engine approach, dropping *AVG* and going with the ubiquitous *Bitdefender* on its own.

The interface is very cool and dark, with a simplified layout featuring chunky buttons for the core operations. Configuration is provided in depth under the covers, in a much more standard format, while logging is stored as plain text but capped at a fixed size in some cases.

Scanning was reasonably nimble, with overheads not excessive either, while RAM use was low, CPU use fairly high, and our set of tasks seemed to skip through extremely quickly. Detection was splendid, with good levels

everywhere, and the certification sets presented no problems either, easily earning *TrustPort* a VB100 award. That brings to an end a brief run of bad luck in our tests, giving the vendor two passes and two fails in the last six tests; six passes and two fails in the last two years. A 'solid' stability rating is also earned, with no issues at all to report.

VirusBuster Professional

Main version: 7.4.68

Update versions: 5.5.1.3/15.0.62.1, 5.5.2.10/15.0.90.0, 7.4.69/5.5.2.11/15.0.102.0, 5.5.2.13/15.0.111.0

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			2

This is a sad day, as what seems certain to be *VirusBuster*'s final appearance in these pages is upon us. The next comparative will be the first since 2007 not to feature a product from the Hungarian company, and only the third since the company first took part in 2000. As testing began

we knew nothing of this of course, and the work itself was fairly unremarkable. The 83MB installer and 78MB updater were simple and fast to operate, updating was as tricky as ever with some runs taking an age to get the job going while others zipped through it in moments. The interface was never a favourite, with clunky controls and oddball layout, but mostly it behaved itself and provided clear and usable logging, providing one remembered to enlarge the size cap of the files created.
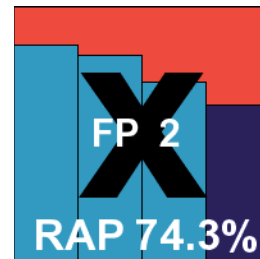
Speeds were OK, overheads likewise not too bad, with average resource use and an average hit on our set of tasks. Detection rates were so-so – not too bad, with good coverage of the WildList sets. In the clean sets though, as expected, a couple of false positives scuppered *VirusBuster*'s chances of winning one last VB100 award. *VirusBuster*'s record has been good though, with 14 consecutive passes in the run up to this test; 43 passes in total from 65 entries over 12 years. The final performance was rated 'fair', perhaps a fitting epitaph.
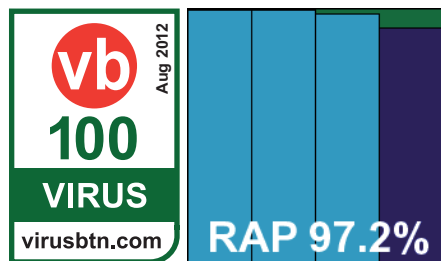
ZeoBIT PCKeeper

Main version: NA

Update versions: NA

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives			0

The final product to discuss this month is from *ZeoBIT*, which last appeared almost two years ago with a very similar solution. Halfway through testing we were contacted by the company to ask about including a completely revamped version of the product in our tests, but as the deadline had long since passed that will have to wait until another time. The version we looked at came as a small downloader file, which fetches the main product as part of the install process – but there can't be a great deal to fetch as everything was completed in under half a minute, with only a couple of clicks. Rebooting was not required. Updating was a little confusing, as the GUI initially claimed we were completely up to date, but on firing off the update process to double-check, we were told that not just definition updates but an entire new product version was available. On each occasion this process still added no more than another minute to proceedings though.

The interface is quite attractive and seems to offer a range of components, including a 'geek on demand' service and a 'one click scan', which includes defragmentation and other checks as well as anti-malware scanning. Configuration is fairly rudimentary for the malware components, but at least covers the basics. Logging is simple and clear.

Scanning speeds were pretty quick, but overheads perhaps just a little on the high side, with RAM use a fraction above average but CPU and impact on our set of tasks both below average. On-access measures over infected sample sets were also rather slow, taking over an hour to do what is in most cases a five-minute job at the most, and the machine became rather bogged down during these tests, but no serious or permanent damage was done.

Detection rates were superb, with some of the highest scores seen this month – in the RAP test they were somehow even higher than those scored by *Avira*, which provided the engine underlying the *ZeoBIT* product. The core sets were no problem at all, and *ZeoBIT* earns its second VB100 award, its previous entry having been in December 2010. We noted a few minor issues with the on-access module under heavy stress, but a 'stable' rating is well deserved.

UNTESTED PRODUCTS

As usual, a few further products took up a fair chunk of our precious testing time this month. Of these, a few were products in development and not suitable for reporting on yet,

a couple were products we were looking over out of interest, and a pair were officially submitted for testing but found too problematic to gather sufficient data on. These were *BluePex*'s *AVware* and *PC Pitstop*'s *PC Matic*, both of which we hope to see reaching a testable standard in the near future.

CONCLUSIONS

As we draw to the close of another epic test, this report will be close to a month late reaching our readers. This is in part due to the high number of entries, in part due to some staffing issues in the test team (which meant the bulk of the testing, results processing and writing work was once again performed single-handed), but mostly thanks to the further expansion in the range of data that is gathered, collated, presented and discussed. We hope readers will appreciate the new table we have added this month, its main focus being the stability rating system; we plan to add a few more columns in future tests.

After a fairly high pass rate in the last comparative, things were back to a more normal ratio this time, with false positives and WildList misses both taking their toll. A few of these were one-off blips, a couple due to unlucky timing, and a couple due to products simply being well below the required standard for certification – but a lot of the issues were with products which really should have been able to pass without difficulty, encountering unexpected problems for no easily explicable reason. In general we saw greater stability than expected though, with only very few products giving us serious problems, which pleased the testing team.

Even as these words are hastily being typed, preparations are under way for the next test, and even the one after that, which should see the first outing of the upcoming *Windows 8* platform; it will be interesting to see how many products are ready for this major release – or at least how many vendors will be brave enough to submit their wares for testing on it just as it emerges publicly.

> **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 7 Professional*, with Service Pack 1, 32-bit edition. For the full testing methodology see http://www.virusbtn.com/vb100/about/methodology.xml.

APPENDIX

We promised a few words on the workings of the new table, and in particular the stability rating system which has been under development over the last few tests. The initial few columns in the new table are fairly self-explanatory, covering a few issues which we have usually mentioned in

passing as part of the write-up: install time is a total measure including both the initial install process and initial updates, taken as an average of the four or more full online installs we do in each test; where reboots are required the time taken to restart is not counted in the total time, and of course times may vary depending on system and Internet connection speeds. Whether reboots are required is recorded in the second column, along with those products which need them only occasionally, after major updates. The third column covers the third-party engines included, where known to us, but cannot cover to what extent in-house technology expands on the protection offered by an engine alone, which may vary considerably from product to product.

The remainder of the table covers the stability rating system. We have tried to keep this as simple as possible for ease of understanding, but it is of necessity rather multi-layered. Essentially we have divided all issues with products into four degrees of severity, labelled 'trivial', 'minor', 'serious' and 'severe', and applied a points scores to each level: one point for trivial issues, two for minor, five for serious and ten for severe. Issue severity is then modified depending on two other factors: under what circumstances the issue occurs and how repeatably it occurs. Bugs that occur in what could be considered normal, everyday use – for example during the speed, performance or false positive tests – are given the full point score, while for those which happen under heavy stress – e.g. during scans of large sets of malware samples, or on-access bombardment with such sets – the point score for that issue is halved. If a bug is consistently repeatable when replaying the same or similar circumstances, the point score is doubled, if it occurs only occasionally there is no modifier, and if it occurs only once and cannot be made to recur the score is halved.

Following this system produces a points value for each bug noted during the testing period. These are totalled to produce a final score, and fitting this score into a fixed scale produces a final rating, ranging from 'solid' for the most reliable products (those which had no issues whatsoever), to 'flaky' for the most bug-ridden – or at least those with the most serious problems. Fixing the boundaries for each rating level was the most difficult task, as we wanted to ensure that products could not be marked down too easily for suffering only minor problems, but also that products could not too easily get away with major and potentially dangerous issues. It may well be that these boundaries are adjusted in the future as we make more use of the system. More details of the underpinnings of the system, including a detailed table of bug classifications, will be included in our full online methodology once a major rewrite is completed, and as usual we welcome comments, criticisms and suggestions from our readers on this and any testing-related matters (email john.hawes@virusbtn.com).