

# virus

## BULLETIN

Fighting malware and spam

### VB100 COMPARATIVE REVIEW ON WINDOWS 8 PRO

#### INTRODUCTION

It was rather an important test this month, with our first look at *Microsoft's* all-new *Windows 8*, and at the products that are available for it. A recent report from *AV-TEST*, a month or so after the public release of *Windows 8*, found some 60 products from 26 different vendors were available for the platform. Our schedules meant that the test deadline fell a few days prior to the public release of the platform, and this seemed certain to pose the vendors a real challenge.

On the deadline day it was clear that several vendors were less than fully prepared for the new platform – or perhaps just short of confidence in their own wares – as a number of our regulars were absent. Of those that did manage to submit products, a few more were clearly far from ready, with bugs and crashes experienced in the process of simply setting the products up for an initial look on the deadline day. This meant that several were excluded from further testing, and also gave us plenty of data for our stability rating system. Of course, with such a new platform it was always possible that a few bugs and errors would crop up that were unrelated to the products being tested, so we had to be a little more lenient than usual when apportioning blame.

After winnowing out a few hopeless cases, our final tally of products was a reasonable 33, giving the team some hope that we might manage to catch up on our schedule and get the test completed before the end of the year. This would of course depend on how malleable and reliable those 33 products proved to be during the course of the test, so as always we settled into the testing area with all fingers firmly crossed, hoping for an absence of the usual horrors.

#### PLATFORM AND TEST SETS

The lab team's initial opinions on *Windows 8* were a mixture of surprise, confusion, occasional grudging

approval, bafflement, bewilderment and general loss of bearings. Designed very much for touch-screen devices, the user interface has been redesigned so radically as to leave seasoned PC users quite at a loss as to where things are. The install process is slick and glossy, and completed in reasonable time, but the process of setting up the test systems was long and slow, mainly thanks to time spent rummaging fruitlessly around trying to find some control which used to be easily accessible. Even something as basic as how to reboot the system took quite a while to figure out, and even when everything had been located and its position carefully memorized, things did not feel at all natural or straightforward. Perhaps with time the new approach will settle in and become second nature, but given that for the most part *Windows* has followed a consistent pattern for many years, it could be a slow and painful process. On top of the layout issues, we also observed some sluggishness in some areas, even on test hardware which seemed fairly high-spec when first acquired a couple of years ago.

Our use of the jazzy 'modern' set-up was thus kept to a minimum, but we did make sure we exercised it fully at the beginning, installing a wealth of popular apps from the nascent *Windows* app store system and adding them all to our clean set for false positive testing. As one of the team recently acquired a new printer, the bulk of the rest of the additions to the clean set this month were printing related, with the download areas of several major hardware providers scoured for useful, popular software which we hoped would not be flagged as malicious by any of our participants. After the usual tidying up and purging of older items, the final set came to just over 700,000 files, measuring around 180GB.

The WildList sets were based on the September lists which were released shortly before our 17 October deadline. Alongside we added our standard set of clean samples used for speed and performance measures, with some minor

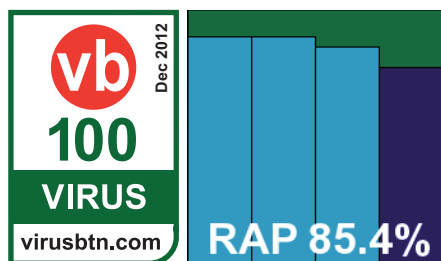
tweaks required to our automation system to ensure a smooth run on the new platform, and a RAP set built with samples first seen in the three weeks prior to the deadline and the week following it, the sets averaging around 20,000 files each after final processing and classification. Response sets were built as needed using the same system, with a set from each day for the week prior to each test run. Testing itself ran throughout November, with the bulk of each of the three runs completed within a week, and the final week of the month and the first few days of December devoted to the remaining RAP and performance tests. As far as possible products were treated in the same manner, running through the same set of processes on matching hardware in much the same order, to ensure equivalence for our stability ratings – the results of which we were particularly interested in on this brand new and highly challenging platform.

### AhnLab V3 Internet Security 9

Main version: 9.0.0.6 (build 462)  
 Update versions: 2012.10.17.30, 2012.11.06.00, 2012.11.12.06, 2012.11.15.00, 2012.11.19.05

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	99.91%
<b>False positives</b>	0	<b>Stability</b>	Solid

We haven't seen much of *AhnLab* lately, with only a single entry before this in 2012, but the company has obviously been keeping



busy, with a major redesign of the product interface seen here for the first time. The installer provided was 133MB and ran through in around a minute with half a dozen clicks required. Updating was performed manually, taking around three minutes on average for the first run. The new GUI is a bit of a departure from the norm, with a rich blue colour scheme and functions divided into four main areas, each represented by a large 'tile' which fitted in nicely with *Windows 8*. Other settings were reached via less prominent links, but were fairly accessible and provided in reasonable detail. A log viewer system allows clear and simple visual access to the logs, which seemed complete and reliable and were easy to export to plain text for more detailed manipulation.

Scanning speeds were rather unpredictable, with one run over the local system partition taking close to two

hours, while others needed little more than 20 minutes. On average, times were slow in the archives set, decent in the set of binaries, and pretty zippy elsewhere. Lag times were not too heavy, while RAM use was low, CPU use a little way above average and the time taken for our set of activities to complete was not bad.

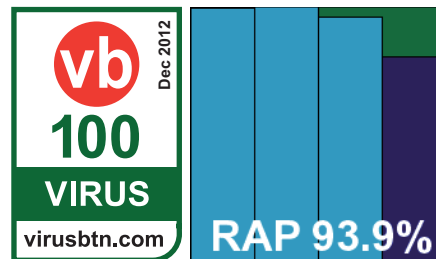
Detection rates were pretty impressive in the Response sets, dropping fairly steeply into the final day, and decent in the RAP sets too, once again the very latest set of samples showing a significant decline. The WildList sets were well covered with no problems in the clean sets either, thus the product comfortably earns our first VB100 award on *Windows 8*. *AhnLab*'s test history is patchy, with now two passes from two entries in the last six tests; four passes and two fails in the last two years. This was the vendor's first exposure to our new stability rating scheme, and with no issues to report it earned a 'Solid' rating.

### Avast Software avast! Free Antivirus

Main version: 7.0.4363  
 Update versions: 121017-1, 7.0.4386/121030-1, 7.0.4388/121109-0

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Fair

A much more regular participant in our tests, it has been more than five years since we ran a comparative without a product from



*Avast*. The current free edition was sent in as a svelte 94MB installer including all required updates for the offline tests, and the set-up process offered an 'express' route which needed only a couple of clicks. The offer to install *Google's Chrome* browser and toolbars is included, and since it is selected by default, this was counted as part of the install itself. With the extra time needed for these additions the main installation took around six minutes, over half of which was taken up by the *Google* components, as far as we could measure. Updates were speedy though, averaging not much more than a minute over several installs. On some occasions, when a major product update occurred, a reboot was required.

The product interface remains very pleasant to look at as well as very simple to navigate and operate, despite

providing an excellent degree of fine-tuning. It appeared to be very stable and reliable throughout testing, although at one point we did experience a blue screen incident. As we were not doing anything particularly related to the product at the time – in fact, simply opening a command prompt window – and the issue could not be reproduced despite our efforts to replicate the exact circumstances, at least part of the blame must be put down to the operating system, but the incident still counts against the product in our stability rating.

Scanning speeds were very fast, as usual, slowing only in the archive set when the scan settings were set to more thorough levels. Overheads seemed fairly low, but this figure will be skewed by the lack of full on-read scanning by default. Resource use was a little above average, but not a great deal, and our set of tasks ran through at a decent pace.

Detection rates were strong, with some excellent scores in the RAP sets, dropping off a little into the proactive week. The numbers were generally high in the Response sets too, with just a couple of off days throwing off the averages a little at either end of the scale. The core sets were dealt with cleanly though, and a VB100 award is easily earned, putting *Avast* on six passes in the last six tests; 11 passes and a single fail in the last two years. Stability was hit by the single freak incident, which was not repeatable, but rather unluckily for *Avast* was just severe enough to edge the rating into the ‘Fair’ category.

### AVG Internet Security Business Edition

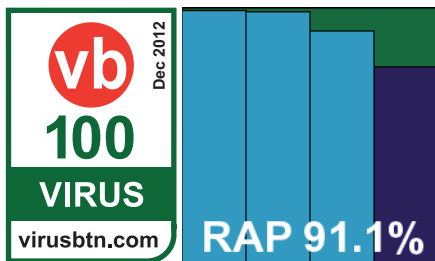
Main version: 2013.0.2741

Update versions: 2614/5834, 2013.0.2743/2617/5875, 2013.0.2793/2624/2889, 2629/2905

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

AVG’s corporate desktop offering also provided an ‘express’ install option, although in this case two or three clicks were needed

to reach this stage and a further two or three afterwards, making for a fairly average amount of user interaction anyway. Options are provided to set the default search provider to AVG’s secure system, and to install a toolbar, but



rather politely these are not checked by default. The install itself, from a 134MB executable with the latest updates rolled in, takes a couple of minutes to run through, with fairly speedy online updates, adding only another couple of minutes; a reboot was required after most update runs.

The interface has been redesigned drastically, clearly aiming to fit in with the tiling style of *Windows 8*. It looks fairly clean and slick, but at times we found it rather tricky to navigate, with key options appearing greyed out and hard to spot thanks to the dark colour scheme. A solid level of configuration was available though, and logging, once found, appeared comprehensive and fairly reliable. However, an option provided regularly to ‘archive’ data seemed to make the logs vanish completely, and no amount of searching could retrieve those accidentally subjected to this action. We also observed some minor freezing of the interface under very heavy stress, which soon righted itself.

Scanning speeds were pretty zippy to start with, and very fast indeed in the warm runs, with overheads likewise improving hugely from an already impressive start. RAM and CPU use were both a shade above average but far from heavy, and our set of activities got through in good time. Detection was excellent – maintaining consistently high levels throughout the Response sets and the first few weeks of the RAPs, and tailing off a little into the later weeks. The core sets presented no problems, and AVG’s new-look product earns a VB100 award with some style, putting the vendor on five passes and one fail in the last six tests; ten passes and two fails in the last two years. With only some very slight issues with the interface and logging, a ‘Stable’ rating is earned.

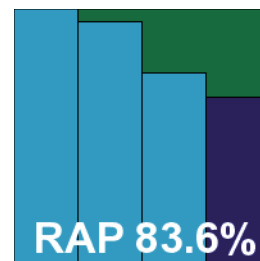
### BeyondTrust Blink Professional

Main version: 6.0.2

Update versions: 1.1.2352, 1.1.2373, 1.1.2352, 1.1.2392

<b>ItW Std</b>	99.81%	<b>ItW Std (o/a)</b>	99.81%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Solid

The company formerly known as *eEye Digital Security* continues to operate seemingly unchanged, with the business version of the *Blink* product much the same as ever. The installer was a fair size at 281MB, including all required data, but it installed fairly speedily, taking only a couple of minutes despite its multiple components – much of the time was spent installing *Visual Studio* runtime software. Updates became noticeably



Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard Wildlist	Extended WildList	FP	Suspicious
AhnLab V3 I.S. 9	100.00%	100.00%	100.00%	99.91%		
Avast Free Antivirus	100.00%	100.00%	100.00%	100.00%		
AVG I.S. Business Edition	100.00%	100.00%	100.00%	100.00%		2
BeyondTrust Blink Professional	99.81%	100.00%	99.81%	100.00%		3
Bitdefender Antivirus Plus 2013	100.00%	100.00%	100.00%	100.00%		
BullGuard Antivirus 2013	100.00%	100.00%	100.00%	99.96%		
Commtouch Command	100.00%	100.00%	99.81%	99.83%	3	1
Emsisoft Anti-Malware	100.00%	100.00%	100.00%	100.00%		4
eScan I.S. Suite	100.00%	100.00%	100.00%	100.00%		1
ESET NOD32 Antivirus 5	100.00%	100.00%	100.00%	100.00%		7
ESTsoft ALYac Enterprise	99.62%	98.38%	99.62%	98.38%		
FileMedic Antivirus 2012*	99.75%	96.98%	99.75%	97.66%	46	
Filseclab Twister Antivirus 8	95.39%	88.72%	95.39%	88.72%	5	16
Fortinet FortiClient Lite	100.00%	100.00%	100.00%	100.00%		
F-Secure Client Security	100.00%	100.00%	100.00%	100.00%		2
F-Secure I.S. 2013‡	100.00%	100.00%	100.00%	99.82%		2
Hauri ViRobot I.S. 2011	100.00%	100.00%	100.00%	100.00%		
Ikarus anti.virus	100.00%	100.00%	100.00%	100.00%		1
K7 Total Security	100.00%	100.00%	100.00%	100.00%	1	
Kaspersky I.S. 2013	100.00%	100.00%	100.00%	99.91%		5
Kingsoft Antivirus 2012	100.00%	100.00%	100.00%	100.00%		
Microsoft Windows Defender	100.00%	100.00%	100.00%	100.00%		
MSecure MalwareSecure	100.00%	100.00%	100.00%	93.29%		1
Norman Security Suite 10	99.87%	99.76%	99.87%	99.76%	1	5
Panda Cloud AntiVirus Free	100.00%	100.00%	100.00%	100.00%		
Qihoo 360 Antivirus	100.00%	100.00%	100.00%	100.00%		1
Quick Heal Total Security 2013	100.00%	100.00%	100.00%	100.00%		
Roboscan Enterprise Solution	99.62%	98.38%	99.62%	98.38%		
Sophos Endpoint Security and Control	100.00%	100.00%	100.00%	100.00%		
SPAMfighter VIRUSfighter PRO	100.00%	86.58%	100.00%	86.62%		2
Total Defense Inc. I.S.	100.00%	100.00%	100.00%	100.00%	1	
TrustPort Antivirus 2013	100.00%	100.00%	100.00%	100.00%		
ZeoBit PCKeeper	99.62%	99.96%	99.62%	99.96%		

\* Full detection of standard list in one out of three runs.

‡ Full detection in place in two out of three runs.

(Please refer to text for full product names.)

slower later in the month as more data had to be pulled down, going from just a couple of minutes in the early runs to close to ten minutes later on when over 250MB was downloaded, but reboots were not required.

The interface is simple and fairly easy to navigate, providing a little more than the basics for the anti-malware component. Logging is reliable and comprehensive, although rather wasteful with large chunks of text repeated multiple times throughout. Scanning speeds as ever were rather slow, and overheads also pretty hefty, but RAM use was fairly low and CPU was above average but not outrageous. Our set of tasks took just a fraction longer than the average for the month.

Detection started well in the RAP sets but declined quite steeply into the proactive week, while Response scores started no more than respectably and also showed a fairly sharp drop as we moved to more recent samples. The clean sets saw only a handful of suspicious alerts, including one for an item of adware and one for an application of some sort which was considered worthy of a mention. The WildList sets were mostly handled well but a single item went unobserved in both modes in all three runs – a problem that has occurred in previous tests and which is still being investigated. As a result, *BeyondTrust* cannot be granted a VB100 award this month, the vendor’s history showing three passes and two fails in the last six tests; seven passes and three fails in the last two years. Stability was faultless however, earning a ‘Solid’ rating.

### Bitdefender Antivirus Plus 2013

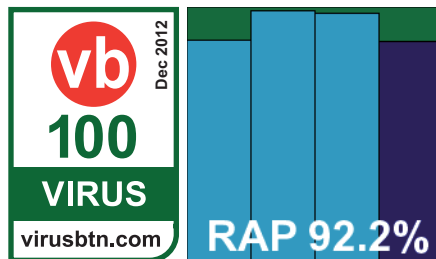
Main version: 16.23.0.1619

Update versions: 7.43739/7645988, 7.43919/7843510, 7.44063/8000253, 7.44094/8001721

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

*Bitdefender* has implemented a fairly drastic overhaul of its image of late too, with its products, logo and slogans all updated to a new style

– however, its performance continues along the same solid lines as ever. The package provided this month – a fairly large 258MB – offers to download the latest version if



available, then provides a single-click, catch-all options page, including the acceptance of a EULA which is not actually displayed. A few further clicks are required after the speedy main install, with options to operate in ‘auto pilot’ mode, and to start a trial, or log into a user account using various shared login systems including *Facebook* and *Google* accounts. When the GUI was up and running, it reported a problem with the web filtering system – something which seemed to persist across a number of installs. The product does not mention that an update might be required in its list of known issues, but manual updates were very rapid indeed, taking no more than 30 seconds, perhaps in part thanks to the process of fetching new install packages when available.

The interface is dark and foreboding, and it is not immediately clear how to go about operating it, but with a little trial and error it soon reveals its secrets, providing a comprehensive range of controls. Logging is stored in an XML format, which appears complete, detailed and reasonable easy to work with.

Scanning speeds were pretty decent, speeding up considerably in some but not all of the warm runs, with overheads very light with the default settings, a little heavier with things turned up to the max. Resource use was on the low side though, with a decent time taken to complete our set of activities too.

Detection was very solid through most of our Response sets, dropping off only slightly into the later few days, and RAP scores were decent for the most part, but in the oldest of the weeks our scans repeatedly crashed out. We tried breaking things down into ever smaller chunks, but inevitably some samples went unchecked as the scanner simply couldn’t get past some of the things that were causing it some nasty problems. This seems to have caused a noticeable dip in the scores for that week, with the others all very impressive indeed. The core sets presented no such issues though, the product sailing through the WildList and clean sets without trouble and easily earning a VB100 award – maintaining *Bitdefender’s* excellent record of 12 passes in the last two years. Stability was shaken somewhat by the crashes under heavy stress in the RAP sets, earning the product only a ‘Stable’ rating.

### BullGuard Antivirus 2013

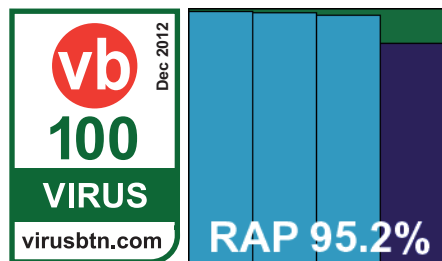
Main version: 13.0.252

Update versions: 13.0.0.30/13.0.0.15/7.43919

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	99.96%
<b>False positives</b>	0	<b>Stability</b>	Stable



Using the *Bitdefender* engine behind the scenes, *BullGuard*'s front end has also had some polishing up in recent months.



The installer measured 163MB this month, and required only a couple of clicks before blasting through its set-up in very quick time. Updates are a little slower, most runs having two stages of downloading and implementation, and in most cases requesting a reboot, sometimes quite a while after the process had apparently completed.

The interface is very minimalist, but reasonably simple to burrow down into to find some decent controls. Responsiveness and stability were pretty good throughout testing; logging is in a rather gnarly XML format, which is easy to access using the product's built-in log viewer system, but on occasions this refused to open larger logs, leaving the user obliged to analyse them manually, which is a less than pleasant task.

Scanning speeds were pretty decent, with some warm runs closely mirroring initial rates while some zipped through in no time at all. File access lags were not too bad, and resource use and impact on our set of activities were also pretty low.

Detection was excellent though, with just a slight decline in the last few days of the Response sets, and the RAP sets were handled superbly, even the proactive week showing an impressive score. The core sets were handled impeccably, earning *BullGuard* a VB100 award this month too, and raising its tally to five passes from five entries in the last six tests, only the annual *Linux* test having been missed, and ten passes from ten entries in the last two years. The log viewer failing to display extra-large logs was the only issue noted, thus a 'Stable' rating is earned.

### Commtouch Command Anti-Malware

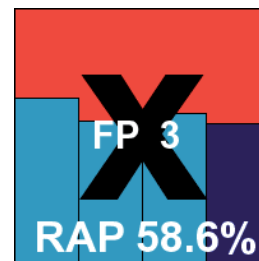
Main version: 5.1.20

Update versions: 5.3.20/201210171259, 201211061437, 201211141016, 201211201350

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	99.81%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	99.83%
<b>False positives</b>	3	<b>Stability</b>	Buggy

Having shown no signs of a redesign for quite a while, *Commtouch*'s product came as the usual tiny 14MB

installer, with offline updates not large either at 28MB. Set-up is fast and simple – there were all the usual steps to click through, but the actual work of putting files into place and so on was over in a flash, and online updates were very speedy too, averaging little more than 30 seconds with no reboots required.



The interface remains pretty basic, providing a reasonable level of control, and giving the user no opportunity to lose their bearings. Logging is straightforward, seemed reliable, and was easy to export from the viewer utility. Speed measures were hampered by crashes when trying to scan the local C: drive – these were repeated every time we attempted the job, so in the end no time could be recorded for this task. Other speed sets were handled better, but we also observed several more crashes in the clean sets. On-demand speeds were fairly slow, with overheads very high on access, and while RAM use was fairly low, CPU use and impact on our set of tasks were both very high indeed.

The scans of infected sets were also hit by numerous GUI crashes, which were adjudged less serious here thanks to the unusual stress levels, but they still slowed things down considerably and hampered our efforts to cover all our sets. Eventually, a reasonably complete set of results were gathered, showing some fairly poor scores in the RAP sets, but much more impressive numbers in the Response sets, at least until the very freshest days, indicating a heavy reliance on cloud scanning to cover the most recent threats. The WildList set was properly dealt with on demand, but on access several items were missed, which may well be for similar reasons. In the clean sets a number of items – including packages from *Canon*, *Lexmark* and *HP* – were flagged as malware. *Commtouch* is thus denied a VB100 award this month by some margin, its test history showing two passes and three fails in the last six tests; four passes and six fails in the last two years. Multiple crashes of the on-demand scanner component, including repeated failure to complete basic checks of the local system drive, tip the stability score over the edge into 'Buggy' territory.

### Emsisoft Anti-Malware

Main version: 7.0.0.10

Update versions: 7.0.0.12

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Product information	Install time (mins)	Reboot required	Third-party engine technology	Stability score	Stability rating
AhnLab V3 I.S. 9	4	N		0	Solid
Avast Free Antivirus	7	S		5	Fair
AVG I.S. Business Edition	4	S		1	Stable
BeyondTrust Blink Professional	8	N	Norman	0	Solid
Bitdefender Antivirus Plus 2013	4	N		3	Stable
BullGuard Antivirus 2013	3	S	Bitdefender	1	Stable
Commtouch Command	1	N	*	16	Buggy
Emsisoft Anti-Malware	1:30	N	Bitdefender	2.5	Stable
eScan I.S. Suite	6	N	Bitdefender	1	Stable
ESET NOD32 Antivirus 5	3	N		1.5	Stable
ESTsoft ALYac Enterprise	6	N	Bitdefender	4	Stable
FileMedic Antivirus 2012	6	S		21	Buggy
Filseclab Twister Antivirus 8	4	N		0	Solid
Fortinet FortiClient Lite	3	N		1	Stable
F-Secure Client Security	12	N	Bitdefender	1.5	Stable
F-Secure I.S. 2013	7	N	Bitdefender	11.5	Fair
Hauri ViRobot I.S. 2011	???	N	Bitdefender	20	Buggy
Ikarus anti.virus	5	N		1	Stable
K7 Total Security	1	N		0	Solid
Kaspersky I.S. 2013	8	N		0	Solid
Kingsoft Antivirus 2012	0:45	N	Avira	8.5	Fair
Microsoft Windows Defender	0:30	N		4	Stable
MSecure MalwareSecure	0:45	N	Ikarus	4	Stable
Norman Security Suite 10	10	YY		0	Solid
Panda Cloud AntiVirus Free	1	N		1.5	Stable
Qihoo 360 Antivirus	2:30	N	Bitdefender	2	Stable
Quick Heal Total Security 2013	2	N		2	Stable
Roboscan Enterprise Solution	7	N	Bitdefender	9.5	Fair
Sophos Endpoint Security and Control	2	N		1	Stable
SPAMfighter VIRUSfighter PRO	1	N	Agnitum <sup>‡</sup>	3	Stable
Total Defense Inc. I.S.	4	YY		12.5	Fair
TrustPort Antivirus 2013	3	N	AVG, Bitdefender	3	Stable
ZeoBit PCKeeper	4	N	Avira	8	Fair

S - Reboot required after some updates

O - Reboot optional, only required for some components

YY - More than one reboot required on some installs

??? - Product never completed install satisfactorily

\* Frisk engine now owned by Commtouch

<sup>‡</sup> VirusBuster engine now owned by Agnitum

(Please refer to text for full product names.)

0 = Solid

0.1 - 4.9 = Stable

5 - 14.9 = Fair

15 - 29.9 = Buggy

30+ = Flaky

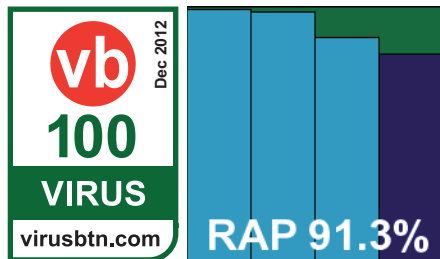
On-demand throughput (MB/s)	System drive*	Archive files			Binaries and System files			Media and Documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
AhnLab V3 I.S.	3.51	2.44	4.35	2.44	28.57	27.26	26.20	25.31	56.55	55.88	47.66	48.27	47.66
Avast Free Antivirus	12.45	227.62	248.32	5.99	41.01	41.45	38.04	25.53	58.29	48.95	50.84	54.22	35.31
AVG I.S. Business Edition	45.37	12.73	1366.06	910.48	38.51	451.06	451.06	63.55	592.06	526.24	115.55	762.62	762.62
BeyondTrust Blink	10.84	3.59	3.58	3.59	5.53	5.46	5.53	26.98	59.57	59.57	40.14	38.78	39.72
Bitdefender Antivirus Plus	15.27	5.29	16.11	5.29	44.47	128.01	44.47	20.28	126.30	44.79	77.82	197.23	77.82
BullGuard Antivirus	16.96	5.66	18.58	5.66	38.04	119.90	38.04	34.04	1114.52	75.18	50.84	635.52	50.84
CommTouch Command	NT‡	6.72	6.41	6.72	17.84	17.38	17.84	20.28	43.45	44.79	37.75	37.14	37.75
Emsisoft Anti-Malware	19.09	6.77	6.50	6.77	20.70	31.11	20.70	25.76	53.82	56.89	79.44	95.33	79.44
eScan I.S. Suite	8.34	17.18	50.12	NA	5.48	56.72	5.48	4.81	114.13	10.63	4.77	55.26	4.77
ESET NOD32 Antivirus	28.89	9.53	25.53	9.53	92.87	282.76	92.87	36.66	1353.38	80.96	152.52	369.02	152.52
ESTsoft ALYac Enterprise	19.35	45.52	248.32	NA	19.55	91.97	19.55	18.69	116.23	41.27	34.98	69.33	34.98
FileMedic Antivirus	10.00	2.03	2.03	2.03	12.97	12.97	12.97	13.88	30.85	30.65	52.96	52.72	50.17
Filseclab Twister Antivirus	12.64	1.90	1820.96	1.90	12.60	1722.55	12.60	9.11	2104.96	20.11	12.50	1144.05	12.50
Fortinet FortiClient Lite	17.02	7.56	9.60	7.56	15.40	15.76	15.40	28.60	63.57	63.15	34.05	33.45	34.05
F-Secure Client Security	36.53	8.20	1820.96	NA	75.18	2104.96	75.18	98.61	6314.88	217.75	346.65	3813.11	346.65
F-Secure I.S.	39.03	8.39	1820.96	NA	131.56	1894.65	131.56	129.99	6314.88	287.04	953.28	3813.11	953.28
Hauri ViRobot I.S.	11.66	4.95	4.83	4.95	21.12	21.14	21.12	11.13	24.57	24.57	15.56	15.56	15.56
Ikarus anti.virus	12.82	5.12	5.20	5.12	14.69	16.08	14.69	22.17	50.25	48.95	49.52	49.95	49.52
K7 Total Security	17.56	7.03	7.09	7.03	14.52	14.86	14.52	62.17	146.86	137.28	86.66	96.94	86.66
Kaspersky I.S.	55.64	3.12	1820.96	3.12	13.73	1457.39	13.73	39.17	6314.88	86.51	28.89	3813.11	28.89
Kingsoft Antivirus	12.15	1.62	1.62	1.62	30.96	30.80	30.96	27.50	60.92	60.72	42.37	42.53	42.37
MS Windows Defender	17.65	3.73	3.32	3.73	15.25	16.22	15.25	27.24	80.62	60.14	34.66	45.76	34.66
MSecure MalwareSecure	16.17	5.39	5.35	NA	14.32	14.74	14.32	20.87	44.68	46.09	32.04	32.59	32.04
Norman Security Suite	17.65	3.88	3.91	3.88	14.86	14.99	19.43	29.79	66.01	65.78	56.91	57.48	56.91
Panda Cloud AntiVirus	16.94	2.46	3.10	2.46	16.75	76.08	16.75	23.63	55.56	52.19	35.97	44.17	35.97
Qihoo 360 Antivirus	17.52	3.06	3.05	1.97	25.57	25.60	16.49	23.06	52.62	39.97	58.66	59.58	47.08
Quick Heal Total Security	32.52	3.79	3.83	3.80	31.11	34.95	30.80	66.51	141.38	131.56	100.35	103.06	81.13
Roboscan Enterprise Soltn	15.67	44.41	227.62	NA	20.91	215.28	20.91	19.07	789.36	42.10	52.23	102.14	52.23
Sophos E.S.C.	16.28	2.29	1820.96	2.29	23.30	2104.96	23.30	30.42	2368.67	67.18	40.14	1634.42	40.14
SPAMfighter VIRUSfighter	14.27	3.16	3.14	NA	15.04	15.02	15.04	19.86	44.58	43.85	26.30	26.60	26.30
Total Defense Inc. I.S.	16.37	3.13	227.62	3.13	11.44	403.09	11.44	14.97	498.57	33.06	74.77	293.32	74.77
TrustPort Antivirus	13.33	6.05	4.71	6.05	15.91	15.88	15.91	31.08	70.17	68.64	46.50	45.94	46.50
ZeoBit PCKeeper	20.47	7.65	7.64	7.65	31.26	30.31	31.26	55.00	120.67	121.44	165.79	161.12	165.79

\* System drive size measured before product installation.

‡ Not tested – product failed to complete scan of C:  
(Please refer to text for full product names.)



After a long partnership with another provider, this month sees the first appearance of a new incarnation of *Emsisoft's* product,



which now features the *Bitdefender* engine alongside the company's own efforts. The fairly large 218MB installer provided few surprises though, following the standard flow and completing in a minute or so, with online updates adding little more than half a minute to the total set-up time. The GUI is little changed, having had a minor refresh a few months ago. It looks fairly good, with a few quirks in the design here and there, but it has a decent layout and a good basic set of controls. It also seemed fairly stable for the most part, with just the occasional wobble under heavy pressure. Recent issues we have experienced with scans crashing out were much less evident this month, with only a couple of incidents encountered.

Scanning speeds were on the slow side over archives and binaries, but pretty speedy elsewhere, with overheads reasonably light across the board, but especially so in our set of miscellaneous files. Resource use was pretty low, and our set of tasks ran through in around average time for the month. Detection was excellent, even in the RAP sets, where we had to use a slightly older version of the detection data thanks to file-corruption issues with the build originally downloaded.

The WildList was well covered, and with only a few alerts on toolbars in the clean sets, a VB100 award is easily earned by *Emsisoft*. The vendor's history is less than edifying, with now two passes and three fails in the last six tests; two passes and eight fails in the last two years. However, given the significant changes under the hood, this should be the start of a new and much more successful era for *Emsisoft*. With only a few problems scanning large infected sets, a 'Stable' rating is earned.

### eScan Internet Security Suite for Windows

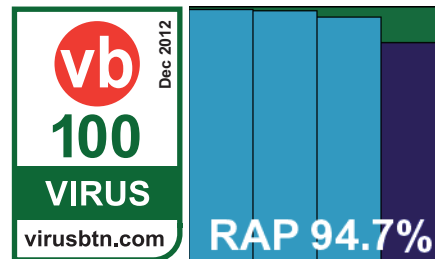
Main version: 14.0.1400.1284 DB

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Another product based around the *Bitdefender* engine, again with a little extra added, *eScan* has been a regular

entrant in our tests for many years, having missed only one test in the last five years. This month saw another fairly dramatic redesign, timed



to coincide with the release of *Windows 8*. The installer provided was a jumbo 397MB, and ran through the standard steps to complete in a minute or so, with updates then taking another half minute to finish off the process. On one occasion the updating GUI opened but then vanished immediately and could not be reopened, but the process seemed to complete successfully and on restarting the main interface all was set back to normal again. No reboot was needed to complete the set-up.

The new interface is another dark, eye-straining thing, with most of the text in grey on a black background, occasionally highlighted in green. Again a tile effect has been worked into the layout to reflect the styling of the new platform, with areas devoted to a set of eight components, each providing some statistics or status information on the component in question (for those with eyes keen enough to make it out amid the gloom). Configuration is impeccable though, much closer to the old familiar style once we get away from the home screen, and logging is clear and complete too. From the configuration screens we could see that this was a late-stage beta.

Scanning speeds were a little on the slow side, but overheads were not too bad, and resource use was fairly low, with a low impact on our set of tasks too. Detection was excellent across the board, with no issues in the core sets and a VB100 award is comfortably earned. The product's test history stands at an excellent six passes in the last six tests; 11 passes and a single fail in the last two years. Only a single, very minor issue with the updating interface was observed, thus the product easily earns a 'Stable' rating.

### ESET NOD32 Antivirus 5

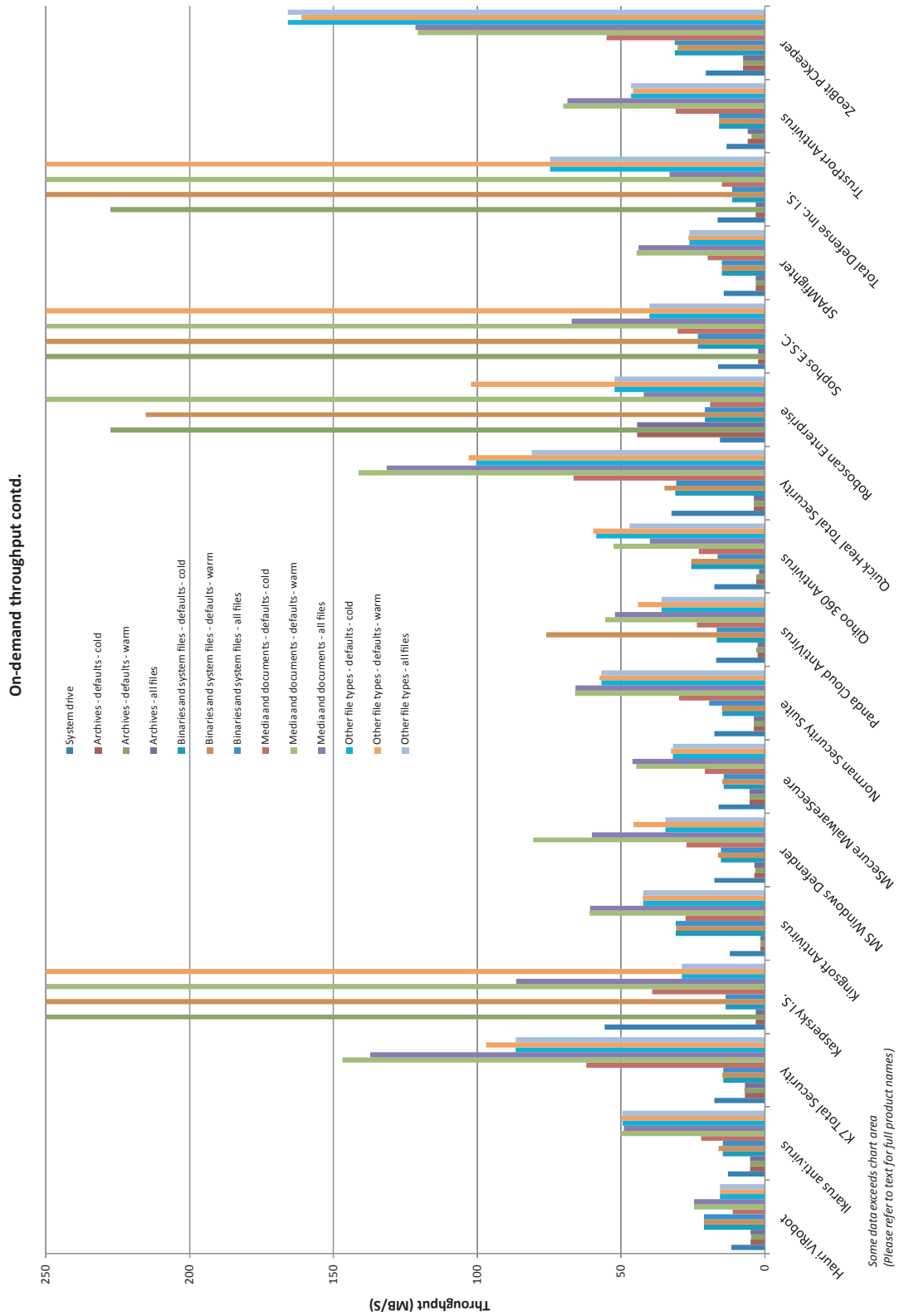
Main version: 5.2.9.1

Update versions: 7597, 7661, 7688, 7706

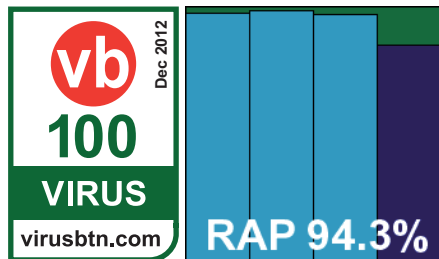
<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Barring any shock upsets, *ESET* should complete a full decade of passing every single *VB* comparative in a few





tests' time. The company's product seemed fully ready for Windows 8, with the standard, compact 65MB installer running through familiar stages to complete within a couple of minutes. Updates added around another minute on average, although in some cases it was less than straightforward to achieve this, as no option to apply a licence was given – the update run simply failed with the message that no licence was in place.



The interface remains unchanged, looking efficient and businesslike, but not unattractive. A vast wealth of fine-tuning is provided under the covers in a reasonably clear and simple way, although there seems to be some duplication of controls and some items we might expect to see appeared to be absent. Operation was mostly stable, but the interface did crash a few times, mostly when under heavy stress such as during on-access runs over large sets of infected samples. Despite the crashes, protection seemed to remain rock-solid throughout. Logging is well displayed in a viewer utility, which again is a little less than obvious in its usage but seemed reliable (although, rather oddly, when asked to export to file, it defaults to saving things to the System32 directory).

Scanning speeds were splendid, almost up to the exemplary speeds of old, with warm runs mostly very quick indeed, while overheads were extremely light. RAM use was very low, CPU use also below average, and our set of tasks ran through in very quick time. Detection was excellent, with reliably high scores throughout the Response and RAP sets, and with the core sets handled perfectly ESET adds yet another VB100 pass to its tally, maintaining its impeccable 12 out of 12 in the last two years, with no fails recorded since 2001 and no tests missed since May 2003. A few interface crashes were observed under stress, but a 'Stable' rating is still well deserved.

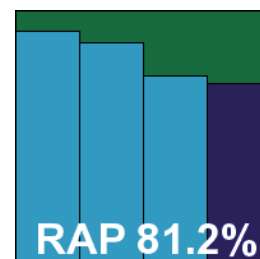
### ESTsoft ALYac Enterprise

Main version: 2.5.0.18

Update versions: 12.4.26.1/451761.2012101113/7.43686/7679200.20121010, 12.4.26.1/455958.2012110618/7.43911/7841561.20121105, 12.4.26.1/457201.2012111318/7.43979/7903168.20121112, 12.4.26.1/458391.2012112018/7.44050/7984770.20121119

<b>ItW Std</b>	99.62%	<b>ItW Std (o/a)</b>	99.62%
<b>ItW Extd</b>	98.38%	<b>ItW Extd (o/a)</b>	98.38%
<b>False positives</b>	0	<b>Stability</b>	Stable

Yet another product using the Bitdefender engine, ESTsoft's offerings have made a number of appearances on our test bench in the last year or so with wildly varying success – some performing excellently, while some, as in the last test, have been too unstable even to make the full report. We hoped for better things this month. The installer measured 153MB and ran through quite a few stages, completing in only a couple of minutes. We have had some issues with the stability of the updater in recent tests, but this time all seemed well, with the process completing within a couple of minutes and indicating successful implementation of data from the current date. No reboot was needed.



The product interface is busy and bustling, but not too cluttered, and a reasonable range of controls is within fairly easy reach. Operation seemed smooth and reliable for a change – the logging system was extremely slow to export, and in a rather bizarre layout, but was apparently complete and fairly readable. Scanning speeds were pretty zippy, with nice light overheads, and resource use was very low indeed, although our set of activities did take a fair amount of time to get through.

Detection rates were a little disappointing though, especially compared to other products this month that are based on the same engine – RAP scores started a little below par and dropped off rather rapidly; Response numbers were distinctly low from the off and plummeted catastrophically into the last few days. At first we assumed this meant that the updates hadn't been as successful as they had seemed, but looking closer at the response numbers showed no indication of this – instead it just appeared that detection data was updating, but still lagged some way behind current. At the time of going to press no explanation for this had emerged from discussions with the developers.

In the core sets, no false positives emerged in the clean set but in the WildList sets, again rather bizarrely, a number of items were missed consistently across both modes and in the three runs, from both the traditional and Extended sets. This meant no VB100 award could be given to ESTsoft this month, putting the vendor on two fails and one pass from three entries in the last six tests (not including aborted attempts); two passes and two fails in the last two years. Stability seemed mostly good, with a few minor judders

in the interface and a few scans aborting thanks to overuse of memory – thus the product just about scrapes a ‘Stable’ rating.

## FileMedic Antivirus 2012

Main version: 1194

Update versions: 1234

<b>ItW Std</b>	99.75%	<b>ItW Std (o/a)</b>	99.75%
<b>ItW Extd</b>	96.98%	<b>ItW Extd (o/a)</b>	97.66%
<b>False positives</b>	46	<b>Stability</b>	Buggy

A new name for our testing rosters, but not an entirely new company, Poland’s *FileMedic* was only formed last year but inherited much of its team from *MKS*, whose old product line *MKS\_vir* is something of a veteran in the industry. Having been quiet for some time, *MKS\_vir* re-emerged a couple of years ago and some products were sent in for us to look at. However, over several attempts few were found stable enough to be included in a full comparative, and only a single fairly disastrous appearance was managed. Now the product returns under a new name and with a new look, and on this occasion we finally managed to cobble together some usable results.

The package submitted measured 105MB, and installed in a fairly standard process which took less than a minute. Updates appeared to be manual only, and ran for around three minutes on average. A reboot is required to complete the installation process, but the message warning of this is rather shy and retiring, fading away after 30 seconds, and is thus easy to miss. The interface is a little basic but clean and crisp, with very little by way of fine-tuning controls, focusing mostly on information rather than options.

Operation was for the most part reasonably smooth and reliable though, at least for the on-demand component, with a few scans crashing out but most making it to completion without too much coaxing. On-access runs through the infected sets seemed to work OK, although clearly not much was detected. However, trying to gather our performance results proved rather difficult: on the first two attempts, the on-access component simply gave up under the pressure (of having lots of clean files accessed, copied around and so on) and shut down – manual restarting proved effective only for a few moments in most cases. Eventually we managed to get all parts to complete with the product awake and active, but this was far from straightforward. The numbers gathered showed some fairly sluggish scan times on demand, with on-access overheads pretty heavy, high resource use and a slow old time of it getting through our set of activities.

Detection rates were not good, with little to get excited about in the Response sets; initial RAP results were

gathered, but it quickly became clear that the build submitted was far from up to date on the test deadline, so the numbers would have been of little relevance. The WildList sets were actually relatively well covered, with not too much missed, but coverage was still some way off perfect, and in the clean sets there were quite a few false alarms – many of them under the same few detection IDs, suggesting that a handful of rogue detections were causing the bulk of the issues. Thus no VB100 award can be granted to *FileMedic* on its first official appearance, but things are certainly looking up and with some more hard work we could see it reaching the required standard in the not-too-distant future. Stability remained something of an issue, particularly with the problems involving the on-access component staying alive. Repeated serious incidents put the score well into the ‘Buggy’ category.

## Filseclab Twister Antivirus 8

Main version: 8.1.5.6709

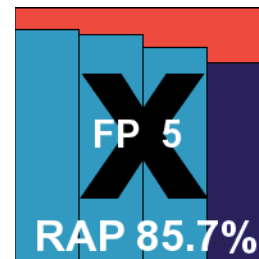
Update versions: N/A

<b>ItW Std</b>	95.39%	<b>ItW Std (o/a)</b>	95.39%
<b>ItW Extd</b>	88.72%	<b>ItW Extd (o/a)</b>	88.72%
<b>False positives</b>	5	<b>Stability</b>	Solid

A slightly more familiar name, but one that still has not quite made the grade to achieve its first VB100 award, *Filseclab* continues to soldier bravely on, showing small improvements from test to test. The latest offering came as a 149MB package, with offline updates measuring a compact 5.4MB,

and ran through the usual steps to install quite quickly. With the initial set-up complete, a brief survey probes the user’s knowledge of security matters, including such questions as ‘have you ever used anti-virus before?’ and a list of terms which you may or may not recognize. Based on the user’s responses, the knowledgeable user is offered a ‘Pro’ mode, while novices are recommended ‘Standard’ mode – this appeared to make minimal difference though, the only change we spotted being the enabling of a ‘Registry Defense’ module in the more advanced mode. While all products saw some prompts for the UAC system during installation, here we saw further prompts when choosing to activate a trial mode, and also when running a manual update, which clocked in at just over two minutes on average for the first run.

The interface has been updated significantly for this latest version, adopting a much more familiar look and feel





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
AhnLab V3 I.S.	19.99	16.88	18.16	NA	16.19	7.43	16.19	10.87	10.57	10.87	11.80	8.48	11.80
Avast Free Antivirus	6.82	3.70	2.07	149.59	1.41	1.03	26.36	17.05	16.90	37.85	10.91	11.03	25.55
AVG I.S. Business Edition	17.30	8.43	1.30	1.30	37.83	0.26	35.70	10.38	0.68	10.84	8.60	0.64	13.24
BeyondTrust Blink	77.68	18.02	18.15	NA	129.09	132.91	129.09	32.95	34.38	32.95	24.14	24.75	24.14
Bitdefender Antivirus Plus	7.82	5.31	1.75	NA	20.34	0.42	20.80	35.80	21.77	38.58	6.16	0.94	6.93
BullGuard Antivirus	6.33	6.13	2.23	239.72	31.78	8.09	41.60	28.72	16.35	35.28	21.67	15.11	26.42
CommTouch Command	64.76	179.19	178.89	172.55	103.31	77.16	59.32	17.65	78.39	75.17	30.52	27.94	26.47
Emsisoft Anti-Malware	5.64	8.81	7.79	35.67	19.59	16.66	85.37	15.02	14.63	132.11	0.68	0.60	73.16
eScan I.S. Suite	14.91	12.25	4.75	15.74	21.01	5.42	12.16	39.03	21.78	41.22	17.14	0.94	13.03
ESET NOD32 Antivirus	6.65	2.94	3.40	NA	8.67	9.46	8.67	25.00	27.00	25.00	3.01	5.10	3.01
ESTsoft ALYac Enterprise	20.16	6.26	1.48	NA	15.10	6.70	15.10	16.84	13.05	16.84	15.07	13.03	15.07
FileMedic Antivirus	51.93	94.15	94.35	94.15	90.60	90.65	90.60	16.36	18.22	16.36	16.40	17.42	16.40
Filseclab Twister Antivirus	43.37	29.60	29.63	140.08	49.68	50.19	48.01	54.88	55.36	98.01	16.38	16.45	71.69
Fortinet FortiClient Lite	19.72	20.64	1.44	20.64	52.93	0.55	52.93	24.58	20.07	24.58	23.99	10.69	23.99
F-Secure Client Security	18.70	12.81	10.38	NA	76.57	21.98	NA	24.57	18.47	NA	9.35	3.82	NA
F-Secure I.S.	15.50	5.74	2.22	NA	59.00	0.57	NA	8.99	0.65	NA	7.58	0.59	NA
Hauri ViRobot I.S.	38.32	6.33	5.71	5.46	41.64	37.50	37.35	16.98	13.46	13.20	10.47	8.45	8.30
Ikarus anti.virus	55.03	189.53	189.00	189.53	57.75	57.83	57.75	37.52	38.01	37.52	15.26	15.30	15.26
K7 Total Security	17.69	35.97	1.27	NA	75.48	22.43	75.48	13.88	0.53	13.88	10.12	0.56	10.12
Kaspersky I.S.	6.92	9.28	8.01	7.84	18.43	17.21	17.82	16.93	14.76	44.81	2.11	0.97	23.58
Kingsoft Antivirus	17.06	16.56	9.49	NA	31.52	26.21	31.52	52.38	32.67	52.38	20.23	20.20	20.23
MS Windows Defender	1.05	5.62	0.85	NA	52.93	0.08	52.93	32.36	21.10	32.36	13.87	0.56	13.87
MSecure MalwareSecure	18.93	2.64	2.20	NA	20.86	15.64	NA	16.22	17.80	NA	11.05	11.46	NA
Norman Security Suite	53.91	14.17	10.73	NA	102.46	47.39	102.46	32.00	21.40	32.00	22.59	8.82	22.59
Panda Cloud AntiVirus	12.69	32.29	8.30	NA	9.74	4.19	NA	30.00	27.00	NA	11.87	11.76	NA
Qihoo 360 Antivirus	0.67	2.02	1.14	28.28	0.78	0.37	0.49	22.91	21.03	20.76	0.85	0.63	0.82
Quick Heal Total Security	8.20	6.50	1.78	NA	33.65	24.73	33.65	10.11	0.38	10.11	7.53	0.74	7.53
Roboscan Enterprise Soltn	8.14	11.65	1.07	NA	40.59	0.10	40.59	28.92	13.81	28.92	6.36	0.50	6.36
Sophos E.S.C.	16.39	7.97	1.77	418.88	41.32	0.65	44.93	23.48	16.65	32.09	19.90	11.03	25.74
SPAMfighter VIRUSfighter	37.23	83.20	83.63	NA	63.38	63.56	64.38	14.87	15.58	46.09	13.94	14.01	36.97
Total Defense Inc. I.S.	37.95	13.76	13.00	NA	35.60	32.68	35.60	28.81	26.32	28.81	15.17	11.79	15.17
TrustPort Antivirus	24.78	13.23	1.46	297.92	66.72	15.17	69.55	30.08	2.27	35.74	18.77	1.89	22.54
ZeoBit PCKeeper	15.39	121.92	1.27	NA	30.57	21.37	30.57	15.57	0.33	15.57	4.66	0.07	4.66

\* System drive size measured before product installation.  
 (Please refer to text for full product names.)

compared to previous iterations. It is sharp and clear, with a decent range of options provided, and seemed easy to navigate. It also ran very stably, with no significant issues to report. Logging is provided with its own display system, and can be exported in a clear, usable manner.

Scanning speeds were distinctly slow in the initial runs, but barely noticeable in the warm runs, while lag times on access were very much on the heavy side. RAM use was low, but CPU use was very high indeed, and our set of tasks didn't get through as quickly as we would have liked. Detection rates were pretty decent in both the RAP and Response tests, but the WildList sets were well short of the level required, and in the clean sets we saw a number of false alarms too, including alerts on items from *Buffalo*, *SAP* and *Adobe* and popular tools such as *WinAmp*, *MySQL* and *Java*.

Thus once again *Filseclab* is denied a VB100 award, but its upward trend continues and the developers must remain hopeful of making the grade fairly soon. The test history for this product shows three entries in the last six tests, five in the last two years, all without success. The developers can be most proud of their stability this month, scoring a perfect zero and meriting a 'Solid' rating.

### Fortinet FortiClient Lite

Main version: 4.3.5.472

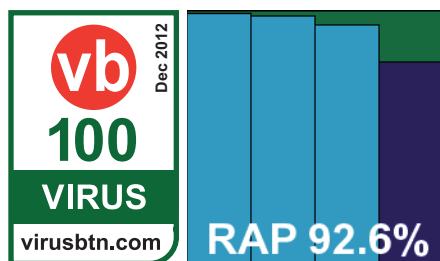
Update versions: 5.026/16.550, 5.026/16.647

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

This month *Fortinet* presented us with a rather different product from what we are used to: its 'Lite' edition.

The install package lived up to its name, measuring just 12MB, with an offline update bundle a slightly heftier 145MB. Set-up was pretty simple, although the option to 'optimize' to the system had us thinking for a moment or two. With this request bypassed, the process completed in little over half a minute. Online updates added a couple of minutes on average.

The interface for this version is a little more cuddly and novice-friendly than *Fortinet's* usual stark, efficient business product line, pared down to remove all the configuration options and other things that the likes of us find useful, but



which are considered too scary for some everyday users. The developers provided us with registry tweaks to disable some of the automatic cleaning and quarantining to speed our tests along, but we didn't have much luck implementing these so we carried on as was, and didn't do too badly. Logging was as complete, clear and readable as ever.

Scanning speeds were not the fastest, but were mostly fairly reasonable, while overheads were a little high at first but much lighter in the warm runs, very sensibly. Resource use was low and our set of activities got through in pretty good time too. Detection tests were a little slower than usual thanks to the extra work of quarantining, and in large sets the product showed a lack of restraint, managing to flood the system drive with all the items it was hiving off and slowing the machine to a sleepy snail's pace.

Things soon returned to normal though, and numbers looked good, with both RAP and Response sets covered excellently at the start, dropping off a little into the most recent samples. The core sets were properly handled, with no false positives or WildList misses, and *Fortinet* comfortably earns a VB100 award with its 'Lite' solution. The test history shows five passes from five entries in the last six tests; nine passes and one fail in the last two years with only the annual *Linux* comparatives not entered. With some bogging down of the system thanks to careless quarantine management noted (but only likely to occur under extreme stress), a 'Stable' rating is earned.

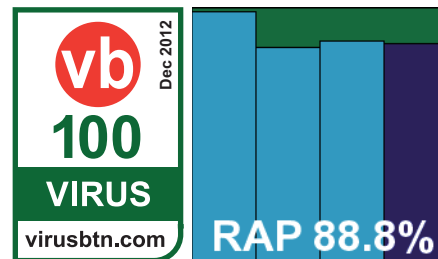
### F-Secure Client Security

Main version: 9.50 build 139

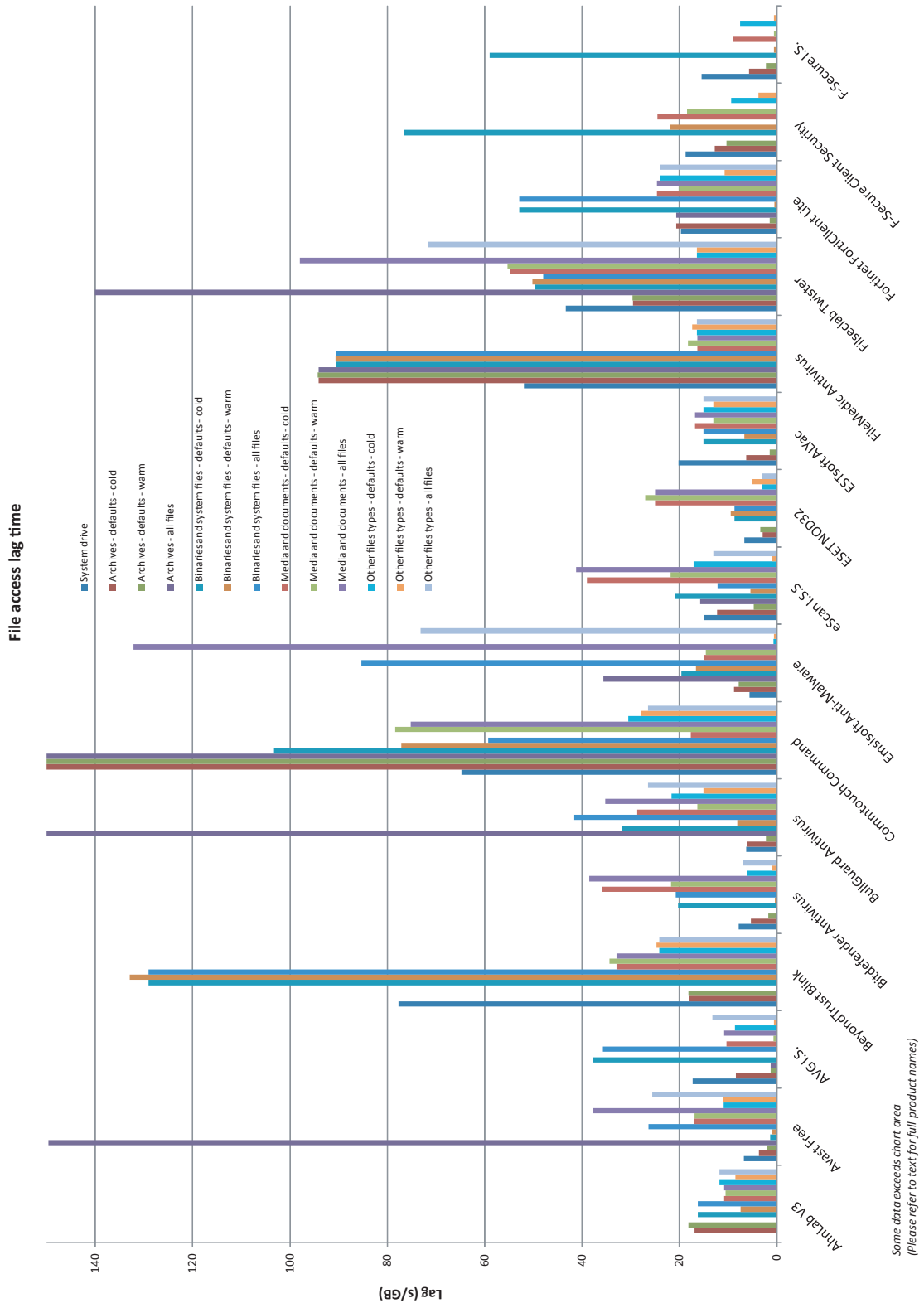
Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

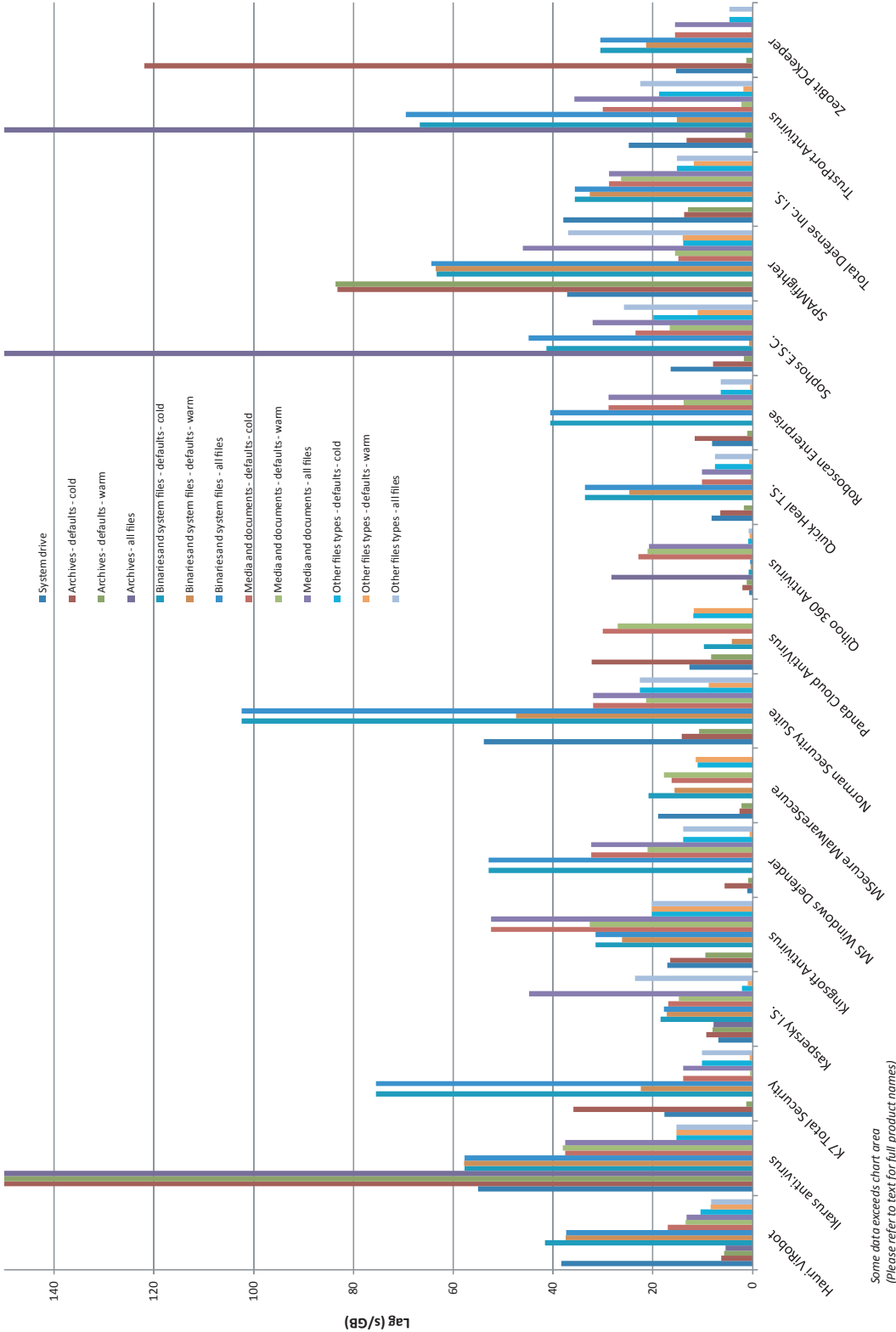
A pair of products once again from *F-Secure*, with the apparent divide being into business and consumer solutions (this appears to be



the corporate offering). The installer provided was a 65MB executable, accompanied by 148MB of updates. Set-up posed the usual questions, completing in a minute or so. An initial update request reported that all was in order on one occasion, with the actual update then starting 30 seconds later; on all runs the update process reported completion



File access lag time contd.



Some data exceeds chart area (Please refer to text for full product names)

within a minute, but it was clear that the product was not fully installed and functional for some time after that – around 10 minutes as far as we could tell.

The interface is familiar from several years of testing: chilly and stark with minimal controls, but fairly well laid out and accessible. The display seemed a little wonky at times though, with some screens showing text cut off halfway down, and as in past tests we had some issues with the system getting a little caught up in itself after the on-access tests, on-demand scans becoming impossible until after a reboot. Logging, as ever, was a little precarious, written only at the end of scans and only storing data from the most recent job, but in a reasonably usable HTML format.

Scanning speeds were easy to gather though, with initial times good and warm runs lightning fast. Overheads showed a similar pattern – initial runs perhaps just a little on the high side but warm runs much improved, although we were unable to persuade the product to scan more than the default list of file extensions in either mode. RAM use was very low but our CPU measurement is a negative figure – a rare occurrence. This is explained by the very long time taken to get through the set of activities – apparently during this period the system was just about idle, thus bringing down the CPU average to well below the figure recorded in the baseline runs where action was rapid and non-stop. Presumably most of this idle time was spent waiting for response from cloud look-up requests.

Detection rates were pretty solid, although a couple of the Response sets fell below the level we would expect from a product incorporating the *Bitdefender* engine, knocking the averages a little. The RAP sets were also below expectations after the first week, although still highly respectable. We could only surmise that these shortfalls were due to problems with logging, as observed in many recent tests.

The WildList sets were well handled though, and with just a couple of items in the clean sets flagged as suspicious by the cloud look-up system, *F-Secure*'s business offering earns a VB100 award without too much fuss. With participation a little irregular of late, it now has two passes and one fail from three attempts in the last six tests; seven passes and one fail in the last two years. A few wobbles in the interface when faced with a little stress testing mean no more than a 'Stable' rating.

### F-Secure Internet Security 2013

Main version: 10.00 build 18410

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	99.82%
<b>False positives</b>	0	<b>Stability</b>	Fair

The second of *F-Secure*'s solutions this month came in a very different format, with nothing more than a tiny 800KB downloader sent in. As product installation can only be done via the Internet, and the decision to submit was made rather late in the day, it was not possible to include it in the RAP tests. Set-up itself was fairly painless, with all the necessary downloading and implementation undertaken in good time, and the main install completed in not much more than a minute and a half. Once again, this appeared to include a successful update, but on checking more closely we found it still (very quietly) reporting a number of components yet to fall into place.

The interface is much the same as the business version, although is complemented by a 'launchpad' component from which one can access several other packages besides the anti-malware solution. Initial test runs proved rather troubling, with the on-access component apparently turning itself on and off again repeatedly during the WildList set. Several runs showed the same pattern of detections and misses. Retrying the same task some time later proved much more successful, but still not quite as complete as we would have liked, while reinstalling a week, and then a fortnight later, the issue seemed to have gone away entirely with no intervention from us – presumably having been spotted and fixed by the developers. Again, logging was not to our tastes, but for on-demand work at least it appeared to be recording complete data, as long as the data was caught and backed up before being overwritten on the next scan. On-access logging seemed to be absent.

Scanning speeds were excellent though, again showing impressive improvements in the warm runs in both modes, but with no option to expand the coverage to include non-standard extensions. RAM use was low, but again the activities time was sky-high – considerably higher even than its sister product – and this meant another negative CPU measurement thanks to long idle periods.

Detection was hard to criticize however, with excellent rates across the board, although sadly no RAP scores could be recorded. The issues in the first on-access run knock the averages down a little, but fortunately for *F-Secure* they only affected the Extended WildList, for which we do not (currently) require full coverage on access. With 100% in the subsequent two runs, and again just a couple of cloud-based suspicious alerts in the clean sets, a VB100 award is merited. Our test history for *F-Secure*'s secondary product line is a little sparse these days, with two passes from just two entries in the last six tests; three from three in the last two years. Some nasty issues were noted in one of





Response tests	Day-7	Day-6	Day-5	Day-4	Day-3	Day-2	Day-1	Average
AhnLab V3 I.S. 9	94.22%	94.90%	96.56%	95.64%	95.09%	93.02%	82.93%	93.19%
Avast Free Antivirus	82.78%	94.43%	94.40%	87.79%	95.06%	90.38%	60.66%	86.50%
AVG I.S. Business Edition	99.62%	98.11%	98.82%	99.01%	98.11%	98.09%	98.44%	98.60%
BeyondTrust Blink Professional	81.49%	85.07%	83.21%	73.81%	76.23%	70.97%	67.67%	76.92%
Bitdefender Antivirus Plus 2013	98.49%	99.10%	99.04%	98.69%	98.02%	95.99%	93.76%	97.58%
BullGuard Antivirus 2013	98.49%	99.09%	99.03%	98.70%	98.00%	95.99%	93.69%	97.57%
CommTouch Command	98.29%	97.79%	97.98%	99.14%	98.85%	94.98%	63.46%	92.93%
Emsisoft Anti-Malware	98.71%	98.98%	99.15%	98.94%	98.38%	96.86%	94.58%	97.94%
eScan I.S. Suite	98.53%	99.17%	99.06%	98.72%	98.02%	96.14%	93.90%	97.65%
ESET NOD32 Antivirus 5	97.47%	97.50%	97.93%	96.28%	95.88%	96.13%	97.11%	96.90%
ESTsoft ALYac Enterprise	80.87%	79.53%	76.90%	77.81%	76.33%	42.94%	38.60%	67.57%
FileMedic Antivirus 2012	31.65%	27.67%	26.97%	32.43%	27.81%	20.72%	17.77%	26.43%
Filseclab Twister Antivirus 8	88.72%	94.35%	96.45%	92.45%	93.32%	84.34%	68.65%	88.32%
Fortinet FortiClient Lite	98.89%	99.37%	99.48%	98.88%	98.84%	95.72%	92.59%	97.68%
F-Secure Client Security	96.20%	81.52%	99.39%	99.12%	91.46%	98.60%	96.65%	94.71%
F-Secure I.S. 2013	98.88%	99.38%	99.39%	99.12%	98.59%	98.60%	96.63%	98.66%
Hauri ViRobot I.S. 2011	89.77%	89.50%	84.54%	85.98%	83.99%	53.80%	54.14%	77.39%
Ikarus anti.virus	99.50%	99.51%	99.65%	99.60%	99.16%	98.29%	93.52%	98.46%
K7 Total Security	72.73%	85.10%	79.74%	73.76%	73.44%	72.26%	45.69%	71.82%
Kaspersky I.S. 2013	96.69%	98.35%	98.10%	97.45%	96.16%	95.10%	94.78%	96.66%
Kingsoft Antivirus 2012	99.40%	99.67%	99.55%	99.64%	99.63%	98.64%	96.59%	99.02%
Microsoft Windows Defender	86.17%	92.44%	90.27%	94.05%	88.12%	89.94%	82.01%	89.00%
MSecure MalwareSecure	99.62%	81.77%	99.56%	99.04%	91.40%	97.74%	91.32%	94.35%
Norman Security Suite 10	98.08%	97.20%	95.24%	94.95%	89.93%	91.30%	89.24%	93.71%
Panda Cloud AntiVirus Free	97.80%	91.40%	88.45%	91.67%	94.74%	95.07%	94.08%	93.32%
Qihoo 360 Antivirus	98.52%	99.16%	99.03%	98.73%	98.01%	95.99%	93.79%	97.60%
Quick Heal Total Security 2013	58.18%	77.15%	78.21%	76.09%	79.54%	66.87%	34.42%	67.21%
Roboscan Enterprise Solution	80.87%	79.53%	76.90%	77.81%	76.33%	42.94%	38.60%	67.57%
Sophos Endpoint Security and Control	98.81%	98.15%	99.26%	98.34%	94.72%	90.73%	75.20%	93.60%
SPAMfighter VIRUSfighter PRO	56.92%	68.87%	70.72%	69.49%	69.61%	69.25%	53.60%	65.49%
Total Defense Inc. I.S.	88.72%	90.40%	89.60%	84.77%	86.36%	76.94%	42.55%	79.91%
TrustPort Antivirus 2013	99.78%	99.89%	99.79%	99.86%	99.73%	99.98%	99.57%	99.80%
ZeoBit PCKeeper	99.30%	99.68%	99.33%	99.24%	99.36%	98.71%	98.98%	99.23%

(Please refer to text for full product names.)

the runs, along with some more trivial wobbles, but as the more serious problems occurred only under heavy stress and were not repeated on later runs they do not totally undermine the stability rating, leaving a score firmly in the middle of the 'Fair' zone.

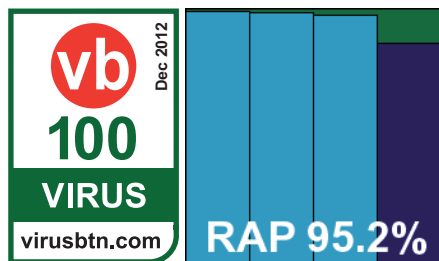
### Hauri ViRobot Internet Security 2011

Main version: 2012-10-17.00 (7645988)

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Buggy

Hauri is yet another user of the popular Bitdefender engine, and another with which we have had a few problems in the past,



most notably with updating not playing ball. This month's submission came as a 187MB installer, which followed the standard path until a quick scan was offered prior to the actual installation. With this step skipped, the whole process took not much over a minute. Updating generally ran for around 30 seconds before halting with a message informing us that we already had the latest updates, but as in several previous tests the version data on the main screen did not change, sullenly insisting that it dated from the initial deadline. No amount of coaxing, cajoling, rebooting and retrying seemed to change this, and the same situation applied on at least four installs on different, fresh hardware each time.

The product interface is fairly shiny and pleasant to look at, and provides some reasonably decent configuration, although it is a little confusing in parts. Apart from the updating fail it seemed to respond well and remained stable under all test scenarios. Logging was comprehensive, reliable and usable. Scanning speeds were a little on the slow side, overheads perhaps a little high in some areas, but resource use was low, especially CPU use, and our set of tasks tripped through very quickly indeed.

Scores were excellent in the RAP sets, closely matching those of most similar products using the same engine, but the Response scores dropped off sharply through the three runs thanks to the lack of functioning updates, resulting in less than excellent averages. The core sets were properly handled though, and a VB100 award is technically earned

despite the absence of any updates through the entire month of testing.

Hauri now has four passes from four attempts in the last six tests; four passes and two fails in the last two years. There wasn't much else to complain about besides the updating issue, but the significance of it, coupled with its repeatable nature, mean a 'Buggy' rating.

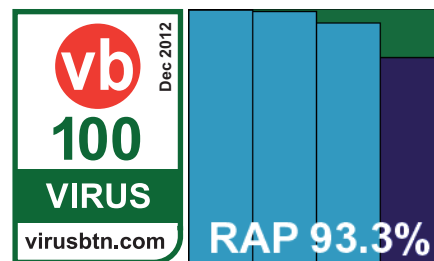
### Ikarus anti.virus

Main version: 2.2.12

Update versions: 1.1.122/82526, 82676, 82733, 82784, 82855

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Having been unlucky with false positives in the last few comparatives, Ikarus rejoins us hoping for a change of fortunes this time.



The install package was a small 23MB, with 89MB of updates provided for the RAP tests. The set-up process includes the downloading and implementation of the .NET framework, so took rather longer for us than it might for those who already have this in place on their systems. The actual set-up of the product itself is fairly speedy, with few surprises along the way other than the option to join a feedback scheme hidden away on a greyed-out screen mainly dealing with update options. Updates were rapid, completing in around half a minute on average, and no reboot was needed to finish off the process.

The interface is pretty basic and a little clunky, providing a limited set of options, but it remained reasonably stable, juddering a little in the most stressful tests. Logging seemed complete and usable. Scanning speeds were a little on the slow side, and overheads rather heavy, with RAM use fairly low but CPU use a little high; our set of tasks got through in quite good time though.

Detection rates were superb in the Response sets, with only the most recent day showing any sign of decline, with excellent scores in the RAP sets too. The WildList set was well dealt with, and with a clean sheet managed in the false positive tests too, Ikarus regains its VB100 certified status with a very impressive performance. The vendor now has

Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities - time increase
AhnLab	3.02%	4.59%	42.12%	15.52%
Avast	10.75%	9.60%	51.73%	35.69%
AVG	10.50%	11.83%	40.82%	26.21%
BeyondTrust	7.39%	6.40%	49.43%	40.37%
Bitdefender	4.79%	4.75%	30.22%	22.12%
BullGuard	7.59%	7.21%	31.60%	16.68%
Commtouch	4.51%	4.06%	90.07%	276.54%
Emsisoft	2.96%	6.05%	15.68%	38.24%
eScan	5.86%	7.39%	24.99%	31.29%
ESET	3.28%	2.27%	17.12%	26.77%
ESTsoft	4.13%	4.51%	4.29%	51.13%
FileMedic	17.13%	16.50%	74.00%	41.18%
Filseclab	2.14%	3.33%	67.73%	52.49%
Fortinet	6.93%	6.54%	27.34%	31.18%
F-Secure C.S.	5.73%	3.90%	-25.99%	86.54%
F-Secure I.S.	7.42%	3.49%	-33.82%	163.17%
Hauri	5.58%	5.28%	1.93%	10.33%
Ikarus	5.96%	5.40%	64.51%	24.14%
K7	8.66%	8.86%	6.39%	36.66%
Kaspersky	11.37%	12.76%	22.22%	36.89%
Kingsoft	7.79%	8.34%	52.29%	33.94%
Microsoft	4.38%	6.52%	15.56%	17.52%
MSecure	2.29%	2.95%	2.21%	4.70%
Norman	6.76%	6.65%	15.84%	24.10%
Panda	3.21%	3.69%	1.39%	19.59%
Qihoo	3.61%	5.64%	4.89%	31.36%
Quick Heal	26.04%	19.92%	1.09%	29.18%
Roboscan	1.36%	3.85%	5.23%	34.01%
Sophos	7.34%	7.37%	15.19%	10.71%
SPAMfighter	5.44%	4.81%	26.88%	50.03%
Total Defense	10.81%	11.13%	18.43%	15.30%
TrustPort	7.94%	10.06%	26.60%	5.64%
ZeoBit	10.17%	10.78%	28.59%	20.35%

(Please refer to text for full product names.)

three passes and two fails in the last six tests; longer term things are not so impressive, with three passes and six fails. With just some minor freezing of the interface under pressure, a 'Stable' rating is well deserved.

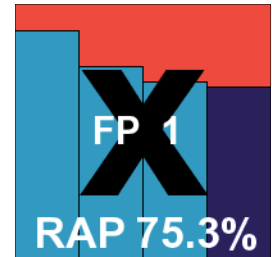
## K7 Total Security

Main version: 12.2.0.151

Update versions: 9.153.7726, 9.154.7822, 9.154.7850, 9.154.7878

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	1	<b>Stability</b>	Solid

K7 tends only to appear in our comparatives on desktop platforms, but has managed to maintain a solid run of performances of late, with an excellent record for stability and a redesigned interface impressing with both its attractive, sensible design and its ruggedness. This month's submission was an 84MB executable, which offered only a single dialog box with a stark 'Agree and Install' button to click. The set-up then took next to no time, followed by a couple of activation stages and a very fast update, the whole job done in little over a minute, including dithering time during the activation step.

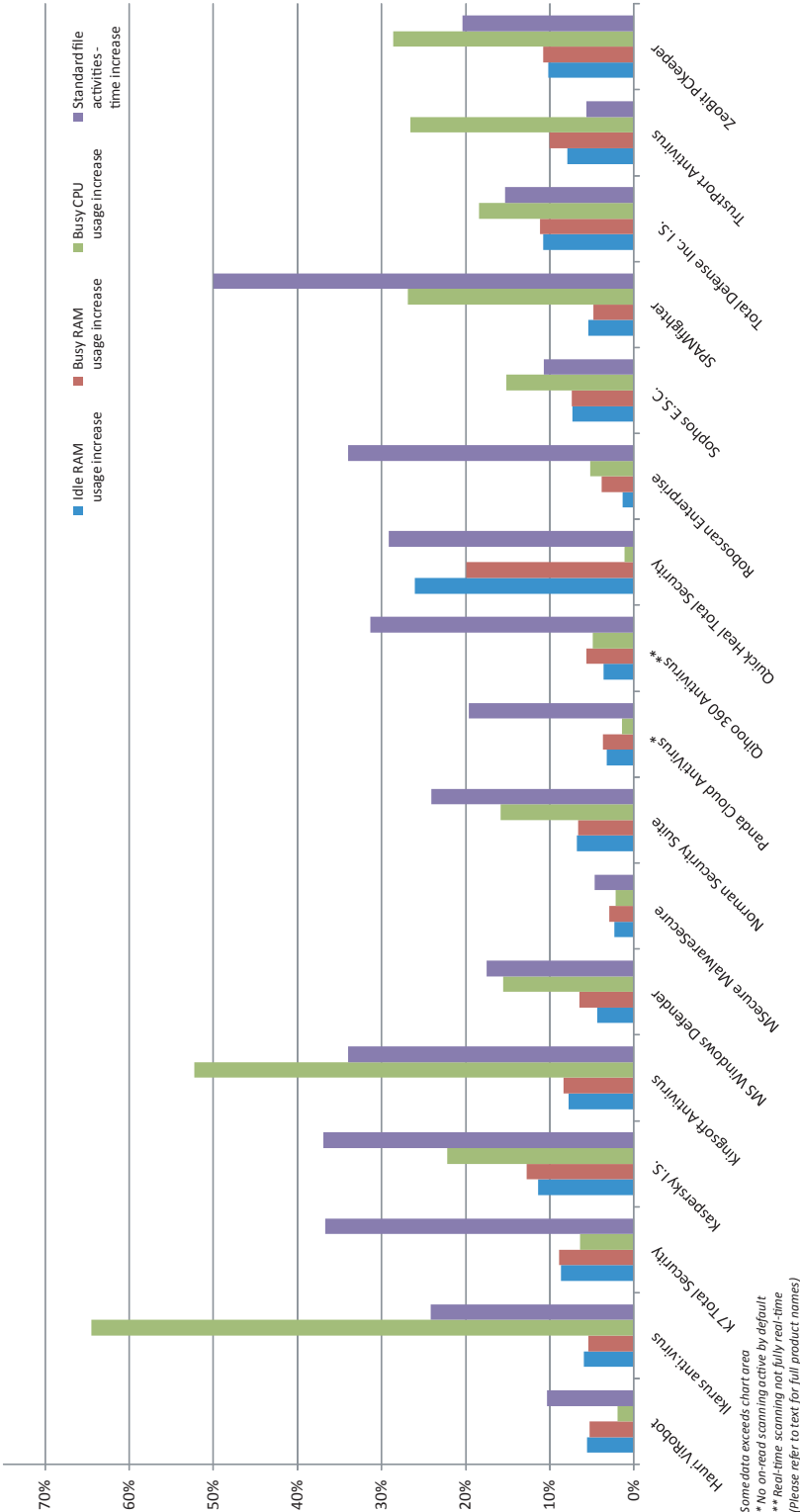


The interface remains pleasing with its military styling, offering a good range of controls in a logical and consistent style. Logging is reliable, complete and usable by both humans and machines. Scanning speeds were a little slow in the sets of archives and binaries, but much faster elsewhere. Overheads reflected this pattern to a degree, with some excellent improvement in the warm runs. RAM use was a little above average, but CPU use very low, and our set of activities got through in reasonable time.

Detection was decent in the RAP sets, with a steady decline through the weeks, and not bad in the Response sets either, the final day showing a steep drop. The WildList sets were well handled, but in the clean sets a single item – part of a package provided by *HP* but apparently built by a third party – was alerted on as a trojan, which was enough to deny K7 a VB100 award this month despite a good showing elsewhere. The company's test history now shows two passes and a single fail from three entries in the last six tests; four passes and one fail in the last two years. No stability problems were observed, earning the product a 'Solid' rating.



Performance measures contd.





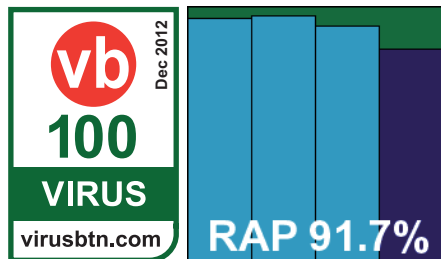
### Kaspersky Internet Security 2013

Main version: 13.0.1.4190 (b)

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	99.91%
<b>False positives</b>	0	<b>Stability</b>	Solid

A much more regular participant, *Kaspersky* rarely misses a test, with an entry in all but two of our comparatives going right



back to 1998. The company’s current product came as a 161MB installer, which was installed and updated online on the deadline day at the request of the developers. The installation process requires minimal interaction and includes a stage of checking for incompatible software, completing in good time. Updates were rather slow though, taking up to ten minutes in some runs. On the last run it was announced that a major new version was available and should be downloaded – the extra several minutes this took added considerably to the overall average set-up time.

The interface has had a few more tweaks since we last saw it, but remains fairly familiar, with its unusual layout and design made a little easier to cope with thanks to regular practice. A comprehensive reporting utility gives access to copious logging data, allowing all manner of manipulation and easy exporting.

Scanning speeds were not too quick initially, but almost instant in the warm runs, with fairly light overheads on access. RAM use was fairly high, CPU use around average, with a reasonable time taken to complete our set of tasks too. Detection rates in the RAP and Response sets were excellent, showing only the slightest decline into the most recent sets, and the core sets were handled with great aplomb, comfortably earning *Kaspersky* another VB100 award to add to its collection. The product now has five passes and a single fail in the last six tests; eight passes and three fails with a single test missed in the last two years. Stability was impeccable, earning a ‘Solid’ rating.

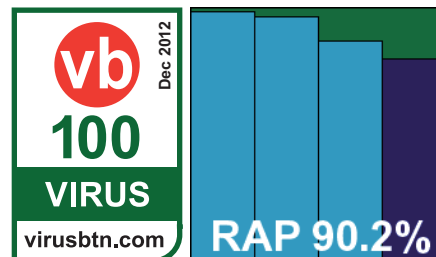
### Kingsoft Antivirus 2012

Main version: 2012.SP3.5.040610

Update versions: 2012.08.23.20

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Fair

*Kingsoft*, hailing from China, was a fairly regular participant in our comparatives for a spell of several years until going



rather quiet around the middle of last year. The vendor now returns with an all-new product, boasting the *Avira* engine under the covers. The 84MB installer ran through very speedily with minimal interaction, with updates also extremely rapid, the whole job completing in little over half a minute on some attempts. Other attempts were slowed down by the updater crashing, which was clearly indicated and seemed fairly graceful, everything working again when it was retried.

The interface is colourful and bright, but provides only minimal controls, running fairly smoothly. Logging seemed clear and usable too, although one run over the RAP sets reported large numbers of detections on screen but far fewer in the actual logs; re-running the scan in chunks proved more effective, implying that rather than simply pruning data to squeeze into size-capped logs, some kind of strange re-counting is performed, resulting in inaccurate and misleading logs.

Scanning speeds were very slow through the archive sets, although settings default to extreme thoroughness, and they were much faster elsewhere. Lag times were a little high but not too intrusive. RAM use was low, CPU use fairly high, with a decent time through our set of tasks.

Detection was excellent, as we have come to expect from the *Avira* engine (*Avira*’s own product is absent from this month’s test thanks to some *Windows 8* compatibility issues that were discovered rather late in the day). The Response sets were demolished, only the most recent day dropping below extreme heights, while the RAP scores started very high indeed but tailed off a little into the later few weeks. The core sets were handled properly, comfortably earning *Kingsoft* a VB100 award for its new-look solution. Our test history covering the old product is split into multiple streams, and is perhaps not particularly relevant thanks to the major change in engine, but it now shows just this single pass in the last year; three passes and a fail in the last two years. Stability was a little shaky at times, with a number of minor GUI hitches and some

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
AhnLab V3 I.S. 9	OD	X	X	X/√	X/√	√	√	√		√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Avast Free Antivirus	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
AVG I.S. Business Edition	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	√	√	X	X	X	X	X	X	√
BeyondTrust Blink Professional	OD	X	1	1	1	1	1	1	8	2	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bitdefender Antivirus Plus 2013	OD	√	√	7	7	√	√	√	7	√	√	√
	OA	X/2	X/2	X/2	X/1	2	X/2	X/2	X/2	1/2	1/2	√
BullGuard Antivirus 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	2/√	X	X	X	1	1	√
CommTouch Command	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2	2	2	2	2	√	2	X	2	2	√
Emsisoft Anti-Malware	OD	√	√	X	X	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
eScan I.S. Suite	OD	X	X	8	7	√	X	X	X	1	1	√
	OA	X/√	X/√	8	8	1/√	1/√	X/√	8	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	X	X	X	X	X	√
	OA	X	X	8	8	X	X	X	X	X	X	√
FileMedic Antivirus 2012	OD	2	√	√	√	√	√	√	√	√	1	√
	OA	X	X	9	9	9	X	9	X	9	1	√
Filseclab Twister Antivirus 8	OD	2	√	√	√	√	1	√	X	√	X	√
	OA	X/2	5/√	5/√	5/√	X/√	X/1	6/√	X	7/√	X	X/√
Fortinet FortiClient Lite	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√	√	√
F-Secure Client Security	OD	X	√	√	√	√	√	√	8	√	X	X
	OA	X	X	X	X	X	X	X	X	X	X	X
F-Secure I.S. 2013	OD	X	√	√	√	√	√	√	8	√	X	X
	OA	X	X	X	X	X	X	X	X	X	X	X

Key:

√ - Detection of EICAR test file up to ten levels of nesting

X - No detection of EICAR test file

X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

\* Detection of EICAR test file with randomly chosen file extension  
(Please refer to text for full product names.)

<b>Archive scanning contd.</b>		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Hauri ViRobot I.S. 2011	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Ikarus anti.virus	OD	7	7	7	7	7	7	7	3	7	7	√
	OA	7	7	7	7	7	7	7	3	7	7	√
K7 Total Security	OD	√	√	√	√	√	√	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kaspersky I.S. 2013	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	X	X	√
Kingsoft Antivirus 2012	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Microsoft Windows Defender	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	X	1	X	√
MSecure MalwareSecure	OD	1	1	1	1	1	1	1	X	1	1	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Norman Security Suite 10	OD	X	√	8	3	√	√	√	8	√	X	√
	OA	X	X	1	3	X	X	X	X	X	X	√
Panda Cloud AntiVirus Free	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X
Qihoo 360 Antivirus	OD	√	√	8/√	8/√	√	√	√	8/√	√	√	√
	OA	√	√	8	8	√	√	√	8	1/√	1/√	√
QuickHeal Total Security 2013	OD	X/2	2/5	1/2	1/2	2/5	X	2/5	1	2/5	X	√
	OA	2	X	2	2	1	X	X	X	1	X	√
Roboscan Enterprise Solution	OD	X	X	8	8	X	X	X	X	X	X	√
	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	√
SPAMfighter VIRUSfighter PRO	OD	2	2	X	X	2	X	2	1	2	2	√
	OA	X/1	X/1	X	X	X/1	X	X/1	X	X/1	X/1	X/√
Total Defense Inc. I.S.	OD	X	2	√	3	4	5	6	7	9	1	xxx
	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/√	√
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.)

unsettling oddities with the logging system, earning no more than a 'Fair' rating.

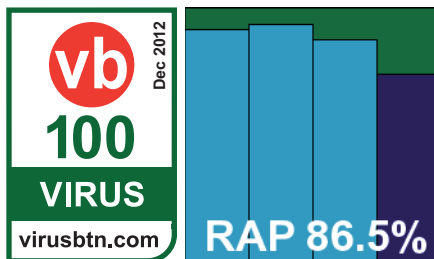
## Microsoft Windows Defender

Main version: 4.0.9200.16384

Update versions: 1.1.8904.0/1.137.1875.0, 1.139.1882.0, 1.1.9002.0/1.141.79.0

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Something old and something very new here. *Microsoft's* malware-battling strategy has been multi-pronged in the past: *Windows Defender*



provided anti-spyware capabilities and was built into *Windows Vista* and *Windows 7*, and offered as a free extra for *Windows XP*. Meanwhile, full anti-virus was provided as a free add-on for home users in the form of *Microsoft Security Essentials*, and prior to that the commercial *OneCare* product. With *Windows 8* we see *Defender* has matured to take on all the anti-malware features of *Security Essentials*, and is bundled in as part of the basic operating system. For the purposes of this test we had to disable its functionality in our base images, to allow other products to install happily and to enable us to record the performance of unprotected systems for our baseline measures. Now we see what happens when it is switched back on.

Installation was of course not an issue, but on each test run when the systems were booted to a fresh image some updating was required; this ran very rapidly, rarely taking more than half a minute to complete. The product interface is very similar to that of *Security Essentials*, slightly pared down with some of the options removed, leaving a very minimal set of controls. Operation is thus pretty idiot-proof, and stability seemed OK, although we did manage to cause a couple of minor interface crashes without exerting any particular stress on the product. Logging is detailed, if a little unfriendly, and on a couple of occasions appeared not to be recording in real time, dropping in some data only after the next system restart.

Scanning speeds were a little slow, with overheads a little high initially but speeding up a lot in the warm measures. Use of RAM and CPU were both well below average, and

our set of tasks ran through very quickly too. Detection was pretty decent in both the RAP and Response tests, with only the most recent set showing a slight decline, and the core sets were properly dealt with, with no WildList misses or false alarms, thus a VB100 award is comfortably earned. As this is, strictly speaking, an entirely new product to our tests it has no history as yet, but looking over the past results for *Microsoft's* corporate and consumer products – entered alternately in most of our tests – we can see a strong pattern of reliable success, with no fails recorded in the last two years. There were a few wobbles noted, but a 'Stable' rating is earned.

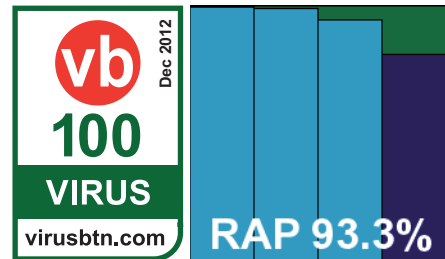
## MSecure Data Labs MalwareSecure Antivirus

Main version: 1.1.107.0

Update versions: 82526, 82696, 82741, 82795























<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	93.29%
<b>False positives</b>	0	<b>Stability</b>	Stable

Another new name for our lists, we first heard from *MSecure Data Labs* just a few weeks prior to the deadline for this test, but the company has



apparently been in business for over ten years, focusing on providing easy-to-use anti-virus and web security solutions. The product incorporates the *Ikarus* engine. The installer provided was compact at 16MB, with updates of 89MB also sent in for use in the RAP tests. The install process follows the standard path and completes very quickly, with updates also extremely speedy, the entire process not needing much more than half a minute to complete.

The interface is simple and angular with a vaguely unfinished feel; it provides some basic controls, and is mostly clear, but in places it uses rather baffling language and at times is less than intuitive. Options to scan archives on access were provided, but seemed to have no effect. Logging of on-access activities is displayed in the interface but seemed impossible to export to file, while on-demand logs appeared to be stored in the root of the C: drive by default. Responsiveness was hit in some of the heavier stress tests, with the GUI and indeed the whole system becoming a little sluggish, and after large scans a reboot was needed to get the interface straightened out, but in normal use it seemed fairly stable.

Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
AhnLab V3 I.S. 9		89.27%	89.43%	85.36%	88.02%	77.45%	85.38%
Avast Free Antivirus		99.46%	99.62%	95.93%	98.33%	80.49%	93.87%
AVG I.S. Business Edition		98.77%	98.20%	90.73%	95.90%	76.59%	91.07%
BeyondTrust Blink Professional		99.76%	94.67%	74.64%	89.69%	65.41%	83.62%
Bitdefender Antivirus Plus 2013		86.84%	98.49%	97.11%	94.15%	86.49%	92.23%
BullGuard Antivirus 2013		98.62%	98.49%	97.11%	98.07%	86.49%	95.18%
CommTouch Command		64.53%	55.94%	58.91%	59.79%	54.92%	58.58%
Emsisoft Anti-Malware		98.72%	97.98%	87.53%	94.75%	81.10%	91.33%
eScan I.S. Suite		98.59%	98.45%	95.93%	97.66%	85.66%	94.66%
ESET NOD32 Antivirus 5		97.19%	98.23%	96.94%	97.45%	84.70%	94.26%
ESTsoft ALYac Enterprise		91.59%	87.37%	74.42%	84.46%	71.43%	81.20%
FileMedic Antivirus 2012		N/T	N/T	N/T	N/T	N/T	N/T
Filseclab Twister Antivirus 8		91.20%	89.19%	84.21%	88.20%	78.22%	85.71%
Fortinet FortiClient Lite		98.53%	97.86%	94.45%	96.95%	79.55%	92.60%
F-Secure Client Security		98.49%	84.29%	86.55%	89.78%	85.82%	88.79%
F-Secure I.S. 2013		N/T	N/T	N/T	N/T	N/T	N/T
Hauri ViRobot I.S. 2011		98.61%	98.47%	97.07%	98.05%	86.47%	95.15%
Ikarus anti.virus		99.48%	98.81%	94.19%	97.50%	80.69%	93.29%
K7 Total Security		89.31%	75.43%	69.30%	78.01%	67.14%	75.30%
Kaspersky I.S. 2013		95.28%	96.23%	92.02%	94.51%	83.41%	91.73%
Kingsoft Antivirus 2012		98.23%	96.19%	86.81%	93.74%	79.59%	90.20%
Microsoft Windows Defender		91.38%	93.14%	87.45%	90.66%	73.93%	86.47%
MSecure MalwareSecure		99.46%	98.76%	94.17%	97.46%	80.68%	93.27%
Norman Security Suite 10		99.35%	94.59%	75.02%	89.65%	66.06%	83.76%
Panda Cloud AntiVirus Free		N/T	N/T	N/T	N/T	N/T	N/T
Qihoo 360 Antivirus		96.27%	94.77%	89.53%	93.53%	81.46%	90.51%
QuickHeal Total Security 2013		70.08%	62.59%	63.71%	65.46%	61.31%	64.42%
RoboScan Enterprise Solution		91.62%	87.56%	74.42%	84.53%	71.43%	81.26%
Sophos Endpoint Security and Control		82.09%	82.73%	76.10%	80.31%	66.79%	76.93%
SPAMfighter VIRUSfighter PRO		57.17%	66.66%	54.92%	59.59%	51.21%	57.49%
Total Defense Inc. I.S.		N/T	N/T	N/T	N/T	N/T	N/T
TrustPort Antivirus 2013		99.81%	99.77%	95.69%	98.42%	85.74%	95.25%
ZeoBit PCKeeper		99.56%	99.48%	96.23%	98.42%	84.94%	95.05%

N/T - Not tested

(Please refer to text for full product names.)

Scanning speeds were reasonable, if nothing too special, while overheads were very light indeed. Resource use was very low and impact on our set of tasks minimal. Detection was excellent, with just the most recent parts of the RAP and Response sets showing a fairly steep drop, and the WildList was well handled with nothing missed. A single adware alert was reported in the clean sets, but no false alarms, and *MalwareSecure* earns a VB100 award on its first attempt, with a promising future ahead of it. Stability of the interface was slightly suspect under pressure, but protection seemed undented, earning a ‘Stable’ rating.

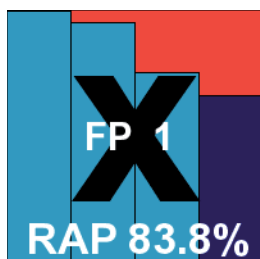
### Norman Security Suite 10

Main version: 10.00

Update versions: 7.00.14, 7.00.16

<b>ItW Std</b>	99.87%	<b>ItW Std (o/a)</b>	99.87%
<b>ItW Extd</b>	99.76%	<b>ItW Extd (o/a)</b>	99.76%
<b>False positives</b>	1	<b>Stability</b>	Solid

The developers at *Norman* promised an all-new product this month, which was provided as a 258MB installer. This ran through quite a number of steps before it finally got down to business, and when it seemed complete it still took some time before the interface was accessible. Running updates was similarly fiddly, with messages that claimed a reboot was needed overlapping with the update process, and a few cycles of reboot-update-reboot-update were needed to get it all set up and working.



The new look is very different, with a proper interface as opposed to the previous browser-based attempt, featuring bright, bold minimalist styling, slightly mimicking the *Windows 8* tile approach, and providing a reasonable basic set of control options. For on-demand scans a simple scanner GUI familiar from previous iterations is still available. Logging is good for the on-demand component, but less usable for the on-access data.

Scanning speeds were not bad at all – a little slow in the archive set where the defaults are set to fairly thorough levels, and overheads were a little high but at least showed some improvement in the warm runs. Resource use was low and our set of activities got through in good time.

Detection was impressive, with excellent figures in the early days of the Response sets, gradually decreasing into the more recent sets, with a similar pattern in the RAP sets where scores dropped steadily through the weeks. The

WildList sets showed a handful of misses though, with the standard set at least fully covered by the time we got to the third of the three passes, and in the clean sets we noted a false positive as well. The developers admitted to having some issues, thanks to a fully rewritten and heavily optimized engine accompanying the new front end, and also let us know that the false alarm had been spotted and fixed before we pointed it out to them. No VB100 award can be given to *Norman* this month, but the work put into speeding things up seems to have paid off and recent improvements in detection seem to continue apace, promising good things for the future. The past looks pretty good too, our test history showing now a single fail and five passes in the last six tests; ten passes and two fails in the last two years. This month’s stability was very good, with no issues reported and a ‘Solid’ rating is earned.

### Panda Cloud AntiVirus Free

Main version: 2.0.1

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

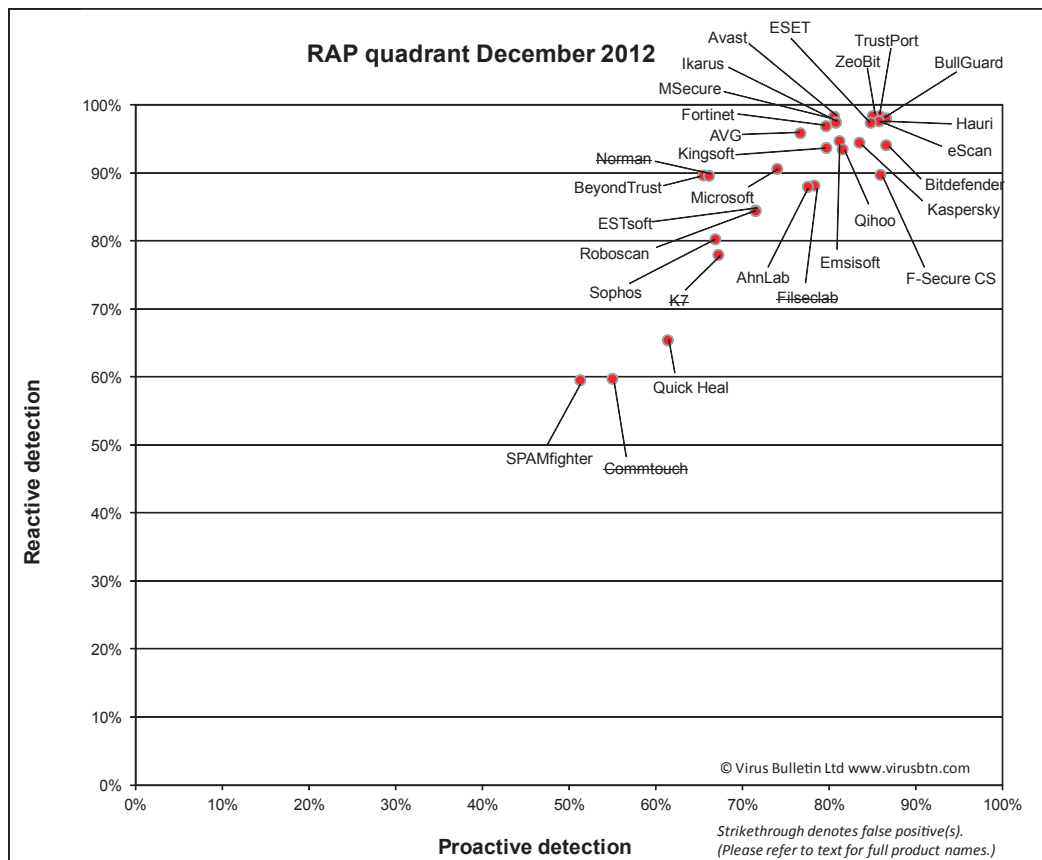
This is *Panda*’s second appearance in our tests this year, after a lengthy absence. There was no physical submission for the free cloud-based solution; instead we simply visited the website, fetched the downloader file and ran it each time we wanted to install the product. Even with this extra step the whole process never took anywhere close to a minute to complete, with minimal fuss.

The product GUI is fairly simple and clear, with little opportunity to get confused thanks to the minimal controls. The default logging is reasonable, but seems to be capped at some arbitrary size limit, making it less than ideal for our needs; an advanced logging option is available, leading to massively more comprehensive logs which seemed perfect, although lacking in some of the detail seen in the standard logs. However, towards the end of testing we realized that these too were limited in size, and that rather than deleting old logs (as seems to be the standard approach), once the limit is hit there is simply no more logging. This meant that some tests had to be re-done, split into smaller chunks, to ensure we could gather all the information required.

Scanning speeds were not bad, and our file access lag time measurement looks excellent, although it should be pointed out that on-read scanning is only implemented for a very limited selection of file types. Resource use







was very low, but again the limited on-read scanning will have impacted this measure, and our set of activities got through in good time. Detection was very good through the Response sets, with no RAP score possible thanks to the entirely cloud-based nature of the product. The core sets were handled well with no issues, earning *Panda* its second VB100 award in as many entries this year. We did have a few wobbles, including a couple of ‘unexpected error’ messages during high-pressure tests, but for the most part things went smoothly, earning a ‘Stable’ rating.

### Qihoo 360 Antivirus

Main version: 3.0.0.3101

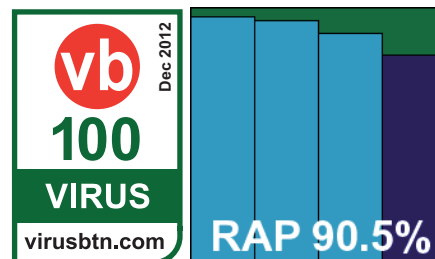
Update versions: 2012-10-17, 2012-11-06, 2012-11-13, 2012-11-20

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

*Qihoo* has become a pretty regular participant in our tests of late, the product including the *Bitdefender* engine. This month’s submission was a 135MB installer, with updates

rolled in. It installed with a single click, completing the job in around half a minute. Updates seemed to be manual only, taking a couple

of minutes on average. The interface has been much the same for a little while, looking sharp and shiny with a fairly straightforward layout and a decent level of configuration. Logging is clear, comprehensive and easy to work with. Scanning speeds were OK – a little slow over archives thanks to thorough default settings, but not bad elsewhere. Overheads were very light, but as usual the real-time mode appears to operate rather differently from the norm, not actually intercepting file accesses but rather checking files as they are accessed and only reporting if they are adjudged malicious some time later; when running our on-access tests over the WildList, some detections were not logged for over an hour after the initial access attempt, with the logs



insisting that access had been denied when it clearly had not. Memory use was rather high in our resource measures, while CPU use was low and our set of tasks took just a little below the average time to complete.

Detection was splendid, keeping pace with others based on the same high-performing *Bitdefender* engine and scoring well in all sets. The core sets presented no difficulties, with just a single item in the clean sets warned about as a possible archive bomb, and a VB100 award is earned by *Qihoo*. The vendor stands on three passes and one fail from four entries in the last six tests; five passes and two fails in the last two years. Stability was decent with a few minor wobbles, earning a ‘Stable’ rating.

### Quick Heal Total Security 2013

Main version: 14.00 (7.0.0.2)

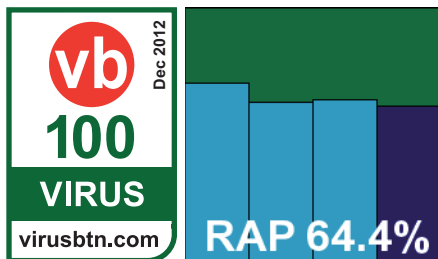
Update versions: N/A

**ItW Std** 100.00% **ItW Std (o/a)** 100.00%

**ItW Extd** 100.00% **ItW Extd (o/a)** 100.00%

**False positives** 0 **Stability** Stable

*Quick Heal’s Total Security* product has been with us for a year or so now, and seemed little changed for the new *Windows* version. The



package provided was a fair size at 326MB, including all required updates. The install process was straightforward and fairly speedy, completing in a minute and a half including a quick scan of vital areas. Updates were also quick, averaging around 20 seconds for the initial run, although one attempt did freeze up, the dialog becoming unresponsive for quite some time.

The interface is bright and colourful, with a slightly unusual but thoroughly usable design and layout, offering a good range of controls. Logging is clear and detailed, but on-access logs cannot be exported, only viewed in the built-in viewer utility. Scanning speeds were a little slow in the archive set despite only minimal coverage of key archive types, but were speedy elsewhere, with light overheads on access. RAM use was very high – the highest recorded this month – but CPU use was barely noticeable, and our set of tasks got through in decent time.

Detection was a little underwhelming – fairly steady through the RAP sets but dropping off rather steeply in

the last few days of the Response sets. The WildList was well covered though, and with no issues in the clean sets a VB100 award is earned. *Quick Heal’s* test history shows three passes and two fails from five entries in the last six tests; eight passes and three fails in the last two years. We noticed a couple of minor issues, including a GUI freeze, but nothing too serious, thus earning a ‘Stable’ rating.

### Roboscan Enterprise Solution

Main version: 2.5.0.18

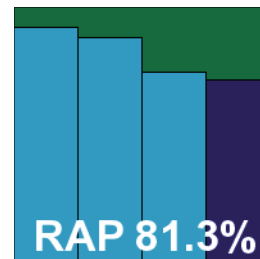
Update versions: 12.4.26.1/451761.2012101113/7.43686/7679200.20121010, 12.4.26.1/455958.2012110618/7.43911/7841561.20121105, 12.4.26.1/457201.2012111318/7.43979/7903168.20121112, 12.4.26.1/458391.2012112018/7.44050/7984770.20121119

**ItW Std** 99.62% **ItW Std (o/a)** 99.62%

**ItW Extd** 98.38% **ItW Extd (o/a)** 98.38%

**False positives** 0 **Stability** Fair

A close cousin of *ESTsoft’s ALYac*, the *Roboscan* submission came at the same time from the same source, and the whole testing experience was pretty similar for the two products. The 157MB package installed in a fair number of clicks, with quite some waiting time, and a couple of attempts saw the progress dialog freezing up completely for over 10 minutes while apparently running a file called ‘install.rse’. They did all complete happily in the end though. Updates were much more reliable than in past tests, with no problems running to completion.



The interface is simple and unfussy, providing a reasonable set of controls and plenty of information. It was mostly reliable, although on a couple of occasions things locked up quite nastily during high-stress scanning work, with messages warning about memory issues and on one occasion the entire system locked up, the screen black and unresponsive and a hard reset required to right things. The logging system is also a little inefficient, routinely taking a very long time to sort its data out into usable form, during which time the product cannot be operated.

Scanning speeds were pretty zippy though, with excellent improvement in the warm runs, and overheads were fairly light – again much better after initial familiarization. Resource use was very low, but our set of activities did take a little while to get through. Detection was again rather disappointing for the *Bitdefender* engine that supposedly underlies things, although update information appeared to

show everything in order. Once again a handful of WildList items were not detected at any point during the test period, meaning no VB100 award for *Roboscan*. The company’s test history shows one pass and two fails from its three entries so far, all of which have been within the last six tests, and with a couple of additional entries aborted thanks to stability issues. There were a number of wobbles here again, including a couple of quite serious ones, but as these mostly occurred only under heavy stress a ‘Fair’ rating is just about earned.

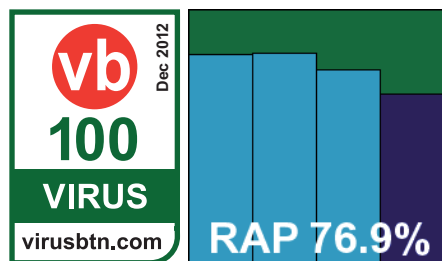
### Sophos Endpoint Security and Control

Main version: 10.2

Update versions: 10.2.0/4.82G/3.36.2,  
10.2.1/4.83G/3.37.2

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

*Sophos* is another contender for the position of the most regular participant in our comparatives, with only two



no-shows in the history of the VB100 scheme. This month’s submission came as a 99MB installer, with offline updates measuring just 9MB; fetching these on the deadline proved a little confusing, as different areas of the company website appeared to be serving different update bundles and we had to double-check to confirm we had the correct ones. The install itself is fairly speedy, although it requires quite a few clicks, highlighted as usual by the offer to remove ‘third party software’ – meaning, of course, other anti-virus products. We also noted that the option to install a firewall component was greyed out, presumably meaning that this part is not yet ready for *Windows 8*. No reboot is needed to complete, and updates are very fast, over in a matter of seconds.

The interface is efficient and businesslike, simple to operate with most options within easy reach and an extreme degree of control is available to those who really want it. Logging is all stored in a single file, which makes sense, and the format is reasonably lucid to the human eye and simple to process automatically. We did note a single odd error message, which occurred when temporarily disabling the on-access component, but it didn’t seem to be more than a minor bug in the interface.

Scanning speeds were a little slow to start off, but zipped through the repeat runs at a very rapid pace, while file access lags were similarly a little high at first but barely noticeable afterwards, at least until we turned the settings up to the max. RAM use was a fraction above average, but CPU use was low and our set of activities got through in excellent time.

Detection was solid, with some excellent scores in the earlier parts of the Response tests, tailing off rather sharply towards the end. RAP numbers declined more gently from a decent starting position. The WildList and clean sets presented no problems, and a VB100 award is well earned, putting *Sophos* on five passes and one fail in the last six tests; ten passes and two fails in the last two years. Just one very minor issue was noted, meaning the product earns a ‘Stable’ rating.

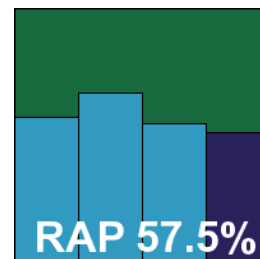
### SPAMfighter VIRUSfighter PRO

Main version: 7.1.274

Update versions: N/A

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	86.58%	<b>ItW Extd (o/a)</b>	86.62%
<b>False positives</b>	0	<b>Stability</b>	Stable

In April, in our most recent *XP* test, we saw the count of products based on *VirusBuster*’s engine almost hit double figures. Less than a year on and how much has changed, with *VirusBuster* no more, the engine now owned and administered by *Agnitum*, and only a single product using it in this month’s test. Brave



*SPAMfighter* submitted its product as a 98MB installer, which required a handful of clicks and completed in 30 seconds. Updates were speedy too, with the whole set-up process complete in not much more than a minute on average.

The interface is bright and reasonably clear, offering some basic controls, and is generally easy to navigate. Stability under pressure remains something of an issue, with the GUI freezing up during large scans or heavy on-access work, but in normal use all seemed fine. Logging is capped at a fixed size, but thankfully it no longer floods log files with unnecessary data, making it fairly usable. Scanning speeds were a little slow, overheads a little high, with RAM use a little below average, CPU use a little above, and our set of tasks a little slower than we would hope.

Detection was slightly disappointing, and a little uneven, but not too bad. The clean sets were handled well, with just a couple of suspicious alerts, and the traditional, replicating part of the WildList was properly covered too. However,

in the Extended list a fair number of items were missed, meaning there is no VB100 award for *SPAMfighter* this month. The vendor now stands at two passes and two fails in the last six tests; seven passes and two fails in the last two years, with things looking on the verge of returning to normal. A few GUI issues were noted under heavy stress, but the score still falls within the ‘Stable’ region.

### Total Defense Inc. Internet Security

Main version: 8.0.0.215

Update versions: 6055.0.0.0, 6063.0.0.0, 6073.0.0.0

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	1	<b>Stability</b>	Fair

It was something of a surprise to see only the consumer offering from *Total Defense* this month – traditionally this one appears in our desktop tests, with its corporate big brother showing up in all tests, but apparently the business edition wasn’t quite ready for *Windows 8* in time for our test deadline. The home user variant is fairly familiar, remaining unchanged in the last year or two, and was provided this month as a 176MB installer. This installs with a single click, running through stages of initial scan, install and update, although on completion some three minutes or so later it seems to still require further updating. This occurs after an initial reboot, and following the update a second restart is then required. The initial scan also alerted on a couple of adware items, with little information provided, and a link in the scan results screen simply leads to an empty search results page on the company’s website.

The interface for the most part is clear and informative though, with configuration limited, but easy to access and operate. Logging is clear and seemed reliable. For the first run at least, scanning speeds were a little slow over binaries and archives, faster elsewhere, but in the warm runs all sets completed very quickly indeed. Overheads were a little high on access, with RAM use fairly high, but CPU use was low and our set of activities got through in good time. One of the scans of clean samples used for speed measures was interrupted by a surprise blue screen incident, which seemed hard to blame entirely on *Total Defense* but nevertheless adds to its stability score. We also noted several scans failing to complete properly, having reported large numbers of detections as they went along but ending with the bewildering statement that nothing at all had been found. Generally, re-running the job proved more successful, but the issue could easily have misled a user into thinking they were safe when the reality was quite different.

Detection was not bad through the Response sets, with no RAP score as the product relies heavily on cloud detection

technology. The WildList was well covered but in the clean sets a single item – an image file which came with software pre-installed on some of the popular *ThinkPad* laptop range – was alerted on as a trojan, apparently thanks to an erroneous cloud look-up result. Thus *Total Defense* cannot be granted a VB100 award this month, the history for the vendor’s consumer product showing two passes and one fail in the last six tests; four passes and two fails in the last two years. A few problems were noted including a blue screen, resulting in a stability rating at the lower end of ‘Fair’.

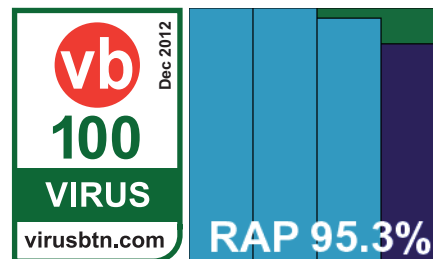
### TrustPort Antivirus 2013

Main version: 13.0.5.5084

Update versions: 13.0.6.5088, 13.0.7.5091

<b>ItW Std</b>	100.00%	<b>ItW Std (o/a)</b>	100.00%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Stable

Another solution including the *Bitdefender* engine, this time in conjunction with *AVG*, *TrustPort* has been a



consistently high performer in our tests for some time now, generally vying with a couple of other multi-engine solutions for the top right-corner spot on our RAP charts. The installer provided was reasonably compact for a multi-engine product, measuring only 216MB, and ran through in a fair few steps in around a minute. Part of the install process was a period of updating, but after the initial reboot that was requested at the end of the set-up, it was clear that things were not fully up to date and more downloads were needed, adding another minute or so on average to the total install time.

The interface is rather unusual, with components scattered among a selection of mini GUIs, but with a little practice it soon becomes fairly simple to navigate. Configuration is provided in reasonable depth, and stability was mostly decent, although one scan did freeze up entirely, refusing to show any results, and had to be re-run. We also observed once again that clear options to extend the size of logs permitted were ignored, with logs being capped at a miserly 1MB, although details of on-demand scans were at least stored elsewhere in a reasonably usable XML format.

Scanning speeds were not bad, overheads a little on the heavy side, but showing good improvements in the warm runs and

only really heavy with the scan settings set more thoroughly than the defaults. RAM and CPU use were both a little above average, but our set of tasks got through in excellent time.

Detection was of course superb – near flawless in the Response sets and very good even in the proactive part of the RAP test. The WildList was covered impeccably, and with no issues in the clean sets either *TrustPort* easily earns a VB100 award, putting it on three passes and two fails in the last six tests; seven passes and two fails from nine entries in the last two years. Stability showed a few little wobbles, but the score falls well within the ‘Stable’ category.

### ZeoBit PCKeeper

Main version: 2.0.103.8660

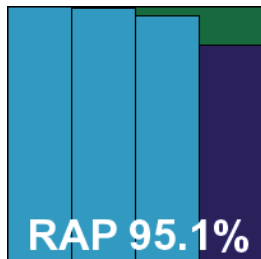
Update versions: 8.2.10.186/7.11.46.170,

8.2.10.192/7.11.49.18, 8.2.10.198/7.11.50.12,

8.2.10.202/7.11.50.126

<b>ItW Std</b>	99.62%	<b>ItW Std (o/a)</b>	99.62%
<b>ItW Extd</b>	99.96%	<b>ItW Extd (o/a)</b>	99.96%
<b>False positives</b>	0	<b>Stability</b>	Fair

We only have a couple of appearances from *ZeoBit* in our records – one very recent and one a couple of years back – but on both occasions we saw some highly impressive performances, with excellent scores thanks to the *Avira* engine underlying the anti-malware part of this fairly comprehensive suite.



When setting the product up on the deadline day we ran into a few problems as *Windows 8* support was still being worked on, and an initial bug meant it refused to install the anti-malware portion on a system which had another product (i.e. the built-in *Windows Defender*) in place. With this worked around, things moved on nicely, and we were later able to try out a more complete version of the installer, which proved pleasant and simple – a ‘one-click’ dialog with options to tweak settings and read EULAs for those who wanted them, followed by a brief slide show during the install itself. This included the slightly garbled and not strictly accurate boast that the anti-virus component has been ‘awarded with VB100 as [one of the] Top 10 solutions in the world’. The process completes in under a minute, after which the opening screen provides a simple wizard for a catch-all check-up of the system. We avoided this and went straight to the anti-malware component, which took a couple more minutes to open, claiming it was ‘gathering data’, but as far as we could tell it was actually installing and updating the *Avira*-based plug-in.

The interface is attractive – busy without seeming cluttered, and offering a range of security, privacy and optimization components, with the offer of human assistance always on hand. The anti-malware area offers a limited but reasonable set of controls, and seemed well laid out. Logging was a little odd, but usable with some fiddling. A few stability speed bumps were hit, including in a portion of the clean set which had been populated with a wide range of popular apps from the new *Windows* app store. Something in here was clearly causing problems, as scans repeatedly froze up and error messages reported problems with the ‘native shim’. Despite repeated attempts, removing items which appeared to be causing the issue, we were unable to get a complete scan of this part of the false positive set, so we cannot be entirely sure that there were no false alarms to report – although it seems improbable.

Elsewhere we managed to gather a complete set of results, and these showed the expected excellent scores in the RAP and Response sets. As far as we could tell given the issues, no false positives emerged in the clean sets, but in the WildList sets a handful of items were not detected, thanks to some problem in the scanner system which the developers managed to fix very speedily once we had reported it to them. This meant no VB100 award for *ZeoBit* this month, but overall a pretty strong showing, with some detection scores to be very proud of. The vendor’s scattered history now shows one pass and one fail from two entries in the last six tests, with only a single additional entry, a pass, a little over two years ago. Stability was far from perfect this month on the new version of *Windows*, with a number of issues noted, earning a rating just within the ‘Fair’ zone.

### UNTESTED PRODUCTS

Given the newness of the platform, we were expecting some products to have trouble this month, and with our deadlines tight we resolved to strike products from the test as soon as it became apparent that severe problems were occurring. Several products were submitted but did not make it to the final line-up; these included solutions from *Coranti* and *Unthreat*, both of which proved too unstable to provide useful results. We will, as always, be working with the developers to help diagnose and correct the issues we observed.

### CONCLUSIONS

Given how close the submission deadline for this comparative lay to the final release date of *Windows 8*, we were expecting to see some issues with compatibility. Despite new versions of major operating systems generally being available to developers months in advance of release, it seems inevitable that some products will be incompletely adjusted and



tested well after the emergence of new platforms. This slow process of adjustment doubtless has a large impact on the slow adoption of new platforms by users. We were thus not surprised to see a few products not arriving on the deadline day, with the absence of some of the largest firms perhaps attributable more to a lack of confidence in their products than to a lack of official support for the new platform.

A handful of the products that were submitted proved too unstable for us to do much with, but those which did work were for the most part reasonably stable. Most had at least a few minor issues, but only a couple were seriously problematic, and even in those cases the issues mostly emerged under the sort of heavy stress that is unlikely to be encountered by real-world users. Hopefully the recent addition of our stability rating system has helped encourage developers to keep a close eye on the quality of their products (or at least, if they feel they are not up to scratch, to prevent them from participating in tests where their shortcomings will be highlighted).

In terms of certifications, this month's pass/fail ratio was close to recent norms at two to one. Looking back over figures jotted down during the last five or six years' worth of comparatives, the long-term average is a fraction over a 70% pass rate, so this month's figures are not too far off. As usual, the most common reason for failing was false positives, but there were also a fair few issues with WildList samples this month, some caused by simple lack of detection and others down to other, internal product issues. With few complex file-infectors in the sets of late we've had fewer problems with the WildList sets, but perhaps the changes required to make products function on the new platform are part of the reason for the increase this time.

In general though, the standard was high this month, and many vendors can justly be proud of their products' performances. Next up, in the new year, will be our annual excursion into the world of *Linux*, which despite the relatively small field of products available invariably throws up some interesting insights. After that we will return to familiar old *Windows XP*, for which we expect to see a far more complete field of products than this month. We will doubtless return to *Windows 8* later in the year, by which time it will perhaps have started to make some penetration into the usage figures and developers will have been forced to pay it proper attention.

#### Technical details

**Test environment:** 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 8 Pro*, 64-bit Edition. For the full testing methodology see <http://www.virusbtn.com/vb100/about/methodology.xml>.

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Dr Morton Swimmer

**Test Team Director:** John Hawes

**Anti-Spam Test Director:** Martijn Grooten

**Security Test Engineer:** Simon Bates

**Sales Executive:** Allison Sketchley

**Perl Developer:** Tom Gracey

**Consulting Editors:**

Nick FitzGerald, *AVG, NZ*

Ian Whalley, *Google, USA*

Dr Richard Ford, *Florida Institute of Technology, USA*

## SUBSCRIPTION RATES

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

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

*Corporate rates include a licence for intranet publication.*

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

- Comparative subscription: \$100

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

**Editorial enquiries, subscription enquiries, orders and payments:**

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

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

Email: [editorial@virusbtn.com](mailto:editorial@virusbtn.com) Web: <http://www.virusbtn.com/>

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

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2012 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2012/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.