



virus

BULLETIN

Fighting malware and spam

VB100 COMPARATIVE REVIEW ON WINDOWS 2008 SERVER R2 SP1

INTRODUCTION

After a rather trying time in the last comparative, we had pinned our hopes on a significant improvement in product performance and behaviour this month. Since this month's was a server test – with many of the products taking part having been designed to protect vital systems – we expected to see far fewer problems here: serious administrators tasked with maintaining pivotal production servers would surely not stand for having them repeatedly crash, freeze or even slow down thanks to wobbly security solutions (and many would take issue with the poorly designed, inaccurate, cryptic or otherwise unusable reporting systems which so regularly cause us problems).

The test deadline was 18 April, which as I write, seems a long time ago. Product submission day passed with few shocks, a medium-sized field of entrants turning up with a few surprise omissions, but the bulk of the regular entrants making an appearance. A single newcomer – a Chinese product with no English translation available – promised some interest, but since we knew it was based on an engine with a solid performance record we were hopeful of a reasonably simple job. As usual, much of the field was made up of OEM and white-label products, and although not quite as dominant as last time around, close to half of this month's submissions included one or other of the two most popular engines for this kind of implementation. In the end, the total number of submissions was 37 – the lowest turnout for a *Windows* comparative since our first look at the *Windows 2008 Server R2* platform two years ago, but still enough to keep us busy.

Just as we were about to make a start on testing, a window opened up for our long-anticipated and well overdue lab move. This proved to be a fairly major undertaking, with the old lab having played host to VB100 testing for close to a decade – but the new space promised more room,

better cooling and power availability, and an all-round environmental improvement compared to the dark and dismal cave we used to call home. The move went fairly smoothly, but almost inevitably there were a number of teething problems getting set up in our new space, and it was more than two weeks before we could get the test underway properly.

PLATFORM AND TEST SETS

Windows 2008 Server R2 has been around for a few years now, as the server equivalent of *Windows 7* first released in late 2009. It has already been the focus of a handful of VB100 comparatives, and has received approval from the lab team for its general air of stability and ease of use. One of few annoyances with its set-up is its insistence on creating a second partition at the start of the main system drive, which makes our re-imaging set-up a little more fiddly than normal. Otherwise, preparing the machines was fairly routine, with nothing beyond the latest available service pack (SP1) and a few handy tools such as archive unpacking and PDF viewing utilities added. As usual, test systems were defragmented and decluttered to make the process of applying a fresh image for each round of testing as rapid and painless as possible.

Test sets were prepared along the usual lines too, with a fairly small set of additions to the clean sets – these focused on business software appropriate to servers, but also included some items which would be more likely to be found in a domestic setting. A number of driver and utility CDs and DVDs received with a fresh batch of machines were also added. After retirement of some older items, the size of the set remained fairly steady at around 180GB, just under 620,000 files. The speed sets and other samples used in our performance measures remained unchanged, and our processes for building the weekly RAP sets and

daily Response sets were also left as they were (once the servers in our new lab space had been coaxed into behaving properly and the daily gathering, classification and storage of new samples was back online). A late start building the RAP sets meant there was more time for items to make their way through to the older test sets, and the ‘Week -3’ set made up more than half the total; weekly sets averaged around 25,000 samples though. The WildList sets were based on the March lists, released a couple of weeks before our deadline. These offered few surprises; once again, a number of items from the Extended list were removed well into the testing period after their appropriateness had been challenged by some reporters.

With much time and effort having gone into getting the lab back up to speed, our plans to extend the data included in this report – such as details of the stability rating system introduced in the last test – were put on hold. After a frenzied period of preparation, we were at least ready to perform our standard set of tasks though, and with no time to waste we got down to the nitty-gritty of putting the products through their paces.

Agnitum Outpost Security Suite Pro 7.5.2

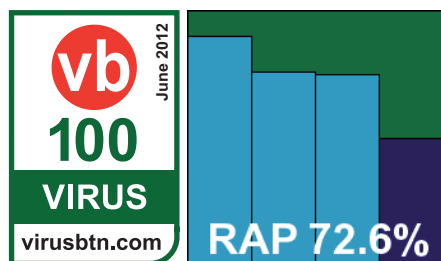
Product version: 3939.602.1809

Update versions: 19/04/2012, 07/06/2012, 11/06/2012, 13/06/2012

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

False positives 0

Agnitum’s Outpost suite will need little introduction to our regular readers, the main features being a renowned firewall and



anti-malware protection based on the *VirusBuster* engine. The product was submitted with latest updates included in a 136MB package. Installation was a little on the slow side, taking two or three minutes to complete when run offline; online updates were fairly zippy though, only adding an extra minute or so to the process. A reboot was required to complete the set-up.

The design is fairly clear and pleasant, with good access to a set of controls that is a little more detailed than the most basic of products. Responsiveness and stability

were generally good throughout, with no serious issues to report. Speed measures showed some reasonable initial scan rates, which increased significantly in the warm runs, with on-access overheads not excessive to start with and showing an impressive improvement once the product had familiarized itself with its surroundings. Performance measures showed some fairly heavy use of memory and very high CPU consumption, with our set of activities taking a long time to complete.

Detection rates were less impressive but still reasonable, with a fairly decent showing in the Response sets. RAP scores were not bad either – in the reactive weeks at least, the proactive week showing a fairly steep decline. The WildList sets were covered perfectly though, and with no issues in the clean sets a VB100 award is comfortably earned. That gives *Agnitum* ten passes from ten attempts in the last two years, with only *Linux* tests missed, and earns the product a ‘solid’ rating for stability.

Avast File Server Security

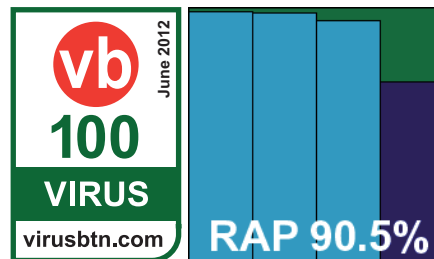
Product version: 7.0.1551/7.0.1617

Update versions: 120418-1, 120531-0

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

False positives 0

Avast’s server solution strongly resembles the vendor’s wildly popular free home-user offerings in most respects.



The package provided weighed in at 95MB including updates, and offered an ‘express’ install mode which got the job done with just a couple of clicks, completing in well under a minute. No reboot was required on initial install, but one of the later updates did request a restart to complete; updates were fairly speedy, making the average set-up time around four minutes.

The interface is attractive and well designed, providing an impeccable range of controls without sacrificing clarity or usability. Responsiveness was generally good, but in the RAP tests the system suffered a single, non-reproducible blue screen incident, which dents the product’s stability rating somewhat – although it did occur in unusually high-stress circumstances.

Speed measures were fairly decent, with very light overheads, at least until the archive scanning settings were turned up to the max, and resource use was fairly low, with an average impact on our set of tasks.

Detection rates were pretty good too, with excellent scores in the reactive part of the RAP sets, the proactive section falling a little short of the very best performers this month but still well ahead of most. Scores in the Response tests were not quite as impressive, but still decent, and with the WildList and clean sets dealt with appropriately, a VB100 award is earned without difficulty. *Avast* now has five passes and one fail in the last six tests; 11 passes in the last two years. Given the single blue screen event, the product earns just a ‘fair’ rating for stability under our new (yet to be fully documented) schema.

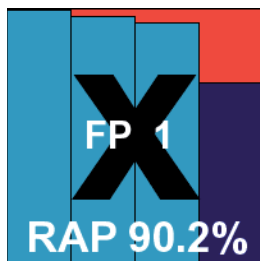
AVG Internet Security Business Edition

Product version: 2012.0.2127
 Update versions: 2411/4940, 2433/5051, 2433/5056, 2433/5064

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

False positives 1

AVG is another big player in the free-for-home-use market, but it is the company’s business solution that is the more regular participant in our comparatives. The package provided measured a sizeable 173MB. Once again, an ‘express’ installation route was offered (accepting all default options) – but three or four clicks are required to get to this stage. The process takes quite some time to complete, the whole job taking more than three minutes, including fairly zippy updates.



The interface itself has had a bit of a refresh of late and looks simpler, crisper and cleaner, with four main areas replacing the large number of overlapping categories previously provided. Customization is available in decent depth, and is pretty simple to navigate and operate, while stability seemed solid throughout testing.

Scanning speeds started off fairly slowly, but the product blasted through the sets once it had had an initial thorough check, and overheads were featherlight throughout. Resource use was pretty low, as was impact on our set of tasks.

Detection rates in the RAP sets very closely mirrored the company’s rival and near-neighbour *Avast*, being excellent

in the reactive parts and very good in the proactive week. Response scores were very impressive too. The WildList was handled well, but in the clean sets a single item was alerted on as a trojan. Closer analysis showed this was an Islamic prayer time notifier, with very high download rates from the popular freeware sites – numbering in the tens of millions in some cases – but apparently no one in the *AVG* user-base had reported a problem with it. Nevertheless, this was enough to deny *AVG* a VB100 award this month, despite an otherwise solid showing. The vendor has five passes and one fail in the last six tests; 11 passes in the last two years. The product merits a ‘solid’ rating for stability.

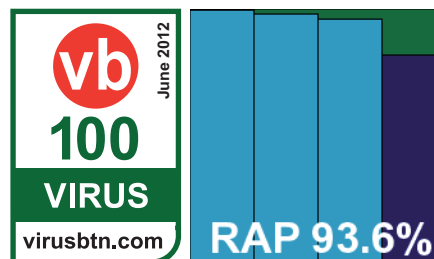
Avira Server Security

Product version: 12.0.0.2038
 Update versions: 8.02.10.48/7.11.27.240, 8.02.10.80/7.11.32.28, 7.11.32.64, 7.11.32.152

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

False positives 0

The third in a trio of popular free solution providers, *Avira* provided a full-blown server solution this month. The base package was only 82MB



including all updates, and with an express option provided it required only a couple of clicks to get going, completing very rapidly with updates taking place in the background (so quickly they were barely noticeable). The whole process was completed in under two minutes, with no need to reboot.

The interface uses the Microsoft Management Console (MMC), and is of necessity a little clunkier and less user-friendly than custom-built ones, but it manages to provide a thorough level of controls nevertheless. Most settings dialogs are provided as pop-outs from the rather wordy and fiddly console system, but navigation and operation was noticeably less smooth and more taxing than others seen this month.

Scanning speeds were pretty decent though, and overheads pretty light, with impressively low use of resources and minimal impact on our suite of tasks. Detection rates were excellent as usual, with a superb showing in the RAP sets and very good scores in the Response sets. With no issues in

Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Suspicious
Agnitum	100.00%	100.00%	100.00%	100.00%		
Avast	100.00%	100.00%	100.00%	100.00%		
AVG	100.00%	100.00%	100.00%	100.00%	1	
Avira	100.00%	100.00%	100.00%	100.00%		
Bitdefender	100.00%	100.00%	100.00%	100.00%		
Bkis	100.00%	100.00%	100.00%	100.00%	18	1
BullGuard	100.00%	100.00%	100.00%	100.00%		
Central Command	100.00%	100.00%	100.00%	100.00%		
Clearsight	100.00%	100.00%	100.00%	99.86%		
CommTouch	100.00%	100.00%	100.00%	100.00%	1	1
Defenx	100.00%	100.00%	100.00%	100.00%		3
Digital Defender	100.00%	100.00%	100.00%	99.86%		
eEye	100.00%	100.00%	100.00%	100.00%		2
Emsisoft	100.00%	100.00%	100.00%	100.00%		4
eScan	100.00%	100.00%	100.00%	100.00%		1
Eset	100.00%	100.00%	100.00%	100.00%		9
ESTsoft	100.00%	100.00%	100.00%	100.00%		
Fortinet	100.00%	100.00%	100.00%	100.00%		
Frisk	100.00%	100.00%	100.00%	99.84%		
G Data	100.00%	100.00%	100.00%	100.00%		
GFI	100.00%	100.00%	100.00%	100.00%		
Hauri	100.00%	100.00%	100.00%	100.00%		
Ikarus	100.00%	100.00%	100.00%	100.00%		
Kaspersky	100.00%	100.00%	100.00%	100.00%		
Microsoft	100.00%	100.00%	100.00%	99.86%		
Norman	100.00%	100.00%	100.00%	100.00%		
Preventon	100.00%	100.00%	100.00%	99.86%		
Quick Heal	100.00%	100.00%	100.00%	100.00%		
Roboscan	100.00%	100.00%	100.00%	100.00%		
Sophos	100.00%	100.00%	100.00%	100.00%		1
SPAMfighter	100.00%	100.00%	100.00%	100.00%		
Symantec	100.00%	100.00%	100.00%	100.00%		79
Tencent	100.00%	100.00%	100.00%	100.00%		
Total Defense	100.00%	100.00%	100.00%	100.00%		
TrustPort	100.00%	100.00%	100.00%	100.00%	1	
UtilTool	100.00%	100.00%	100.00%	99.86%		
VirusBuster	100.00%	100.00%	100.00%	100.00%		

Please refer to text for full product names.

any of the core certification sets, a VB100 award is earned with flying colours. Recent tests show a flawless record of 12 passes in the last two years, and in this case stability was also flawless, earning the product a ‘solid’ rating.

Bitdefender Security for File Servers

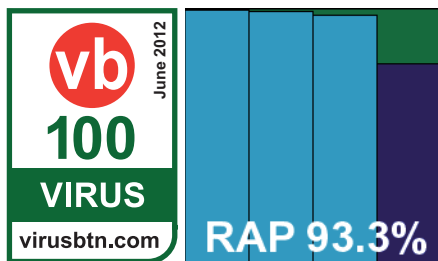
Product version: 3.5.20.1

Update versions: 7076661, 7263693, 7270145, 7280998

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

False positives 0

Another full server solution, and again the MMC is used as the basis for the product interface. The 176MB set-up package ran through a fair



number of steps, with updating and (even more unusually) reporting of incidents back to base both switched off by default. The process took a couple of minutes to complete but updates were reasonably fast and only took an extra minute or so.

The interface is about as well designed as it could be given the underlying MMC system, with some good use of colour and large, clear tabs separating functions. A very good level of configuration is provided. Scanning speeds were a little slow in some areas but very fast in others, while overheads started off fairly heavy but improved greatly in the warm runs. RAM use was fairly low, CPU use closer to average, and impact on our set of activities was noticeable, but far from extreme.

Detection rates were once again superlative, with a splendid showing in the RAP and Response sets. The WildList sets were covered impeccably, and with no issues in the clean sets another VB100 award is well deserved. With all of the last six tests passed, *Bitdefender* has 11 passes and a single fail in the last two years, and merits a ‘solid’ stability rating.

Bkis Bkav Home Plus x64

Product version: 3286

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 18

A much less familiar product, *Bkis* is based in Vietnam and has made a few scattered appearances in our tests, the last of which was a little over a year ago. On the last few occasions we saw some distinctly odd results, with detections apparently depending on whether others were made in the same scan, and logs being adjusted and rewritten retrospectively so that results would differ if logs were looked at during or after a scan job. This time the product came as a jumbo 354MB installer, which seemed to run with only a single click, completing very rapidly but requesting a reboot to complete. On restart, the product interface opened and immediately suggested another restart was needed. Updates also seemed a little problematic, with the interface insisting the latest definitions had been acquired, but the version information and date of the definitions remaining constant, even several months after the initial installer was downloaded.

Testing itself was fairly straightforward, the product’s bright orange interface providing little by way of configuration but seeming to remain stable and responsive throughout testing. Scanning speeds were a little on the slow side, and overheads fairly hefty, with reasonable RAM use but high use of CPU cycles and an above average impact on our set of tasks.

Detection rates in the Response sets looked very impressive, despite our worries over whether updates had worked properly, and the WildList sets were dealt with very well too. In the clean sets however, a number of false alarms emerged, many of them simple autorun configuration files from a selection of legitimate CD back-ups included in our clean sets, but also including components of software packages from major providers such as *IBM*, *Citrix* and *LG*.

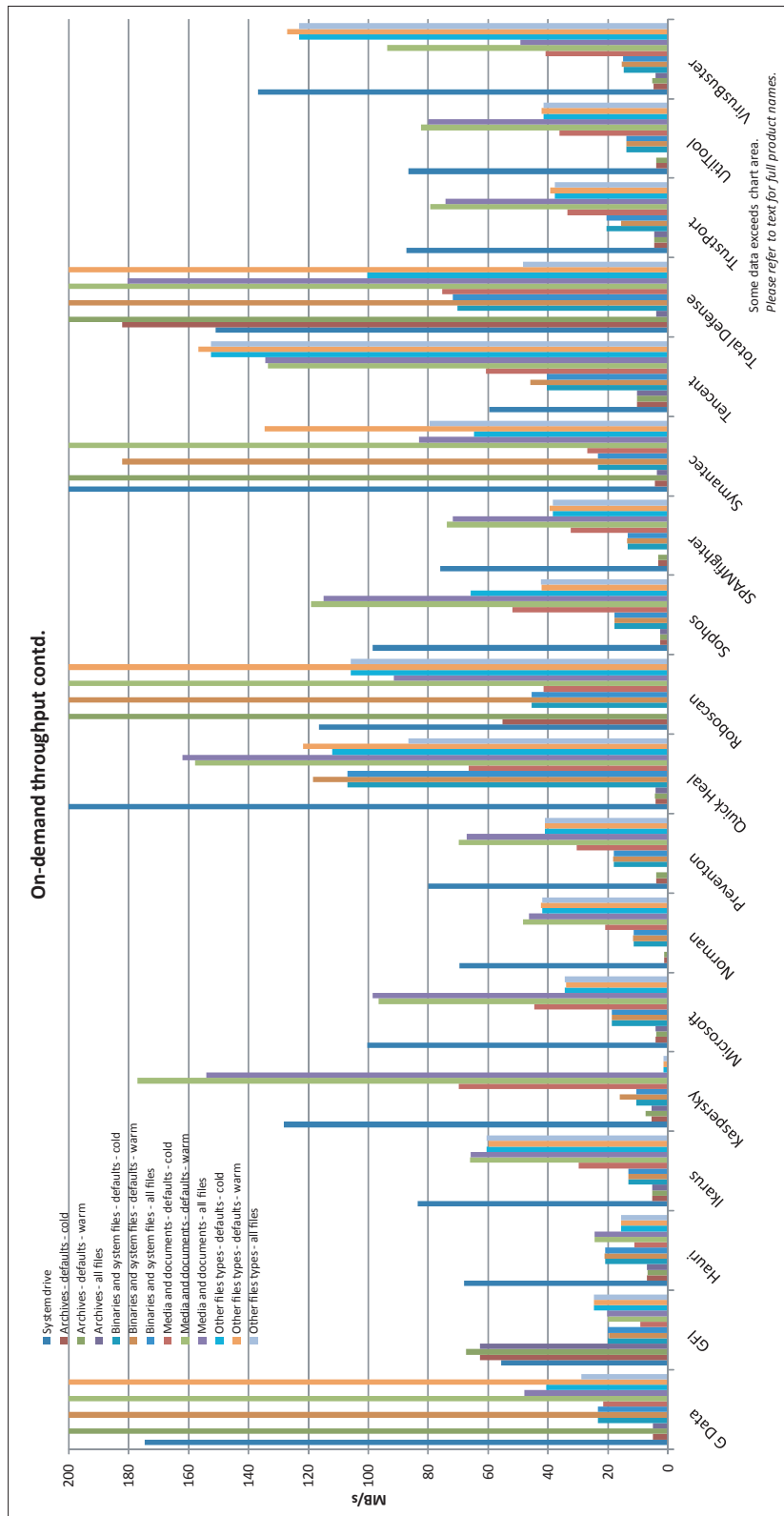
On contacting the developers, it was suggested that changes made to the product to disable automatic disinfection (to help speed along our tests) had in some way broken the logging component, causing it to erroneously log these items as detected, and it was pointed out that if scanned in isolation these files would not be alerted on. This was confirmed, but we also observed that if other clean items were interspersed among the RAP sets, many of them would now be detected as malicious, while some items in the RAP sets would no longer be detected. This complication led us to strike the RAP results out entirely as unreliable. Further discussions with the developers revealed that the ‘test’ version of the product provided to us also used different update servers from those used by real customers, which would not necessarily contain the same detection data available in the real world. This seemed to render our results considerably less than representative of the product’s true performance, and they should thus be taken with a hefty pinch of salt.

On-demand throughput (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum	60.12	2.88	1820.96	2.88	16.62	1894.65	16.62	28.31	3157.44	62.52	32.31	1906.56	32.31
Avast	100.52	8.17	8.09	8.17	30.51	31.06	30.51	37.14	82.01	82.01	47.08	49.10	47.08
AVG	172.82	1.69	1820.96	1.69	33.59	2104.96	33.59	17.99	2104.96	39.72	21.18	1906.56	21.18
Avira	174.33	6.11	6.11	6.11	33.06	33.35	33.06	25.31	56.05	55.88	48.27	48.68	48.27
Bitdefender	119.07	5.13	5.23	5.13	24.48	25.43	24.48	57.20	128.88	126.30	108.95	107.92	108.95
Bkis	76.06	79.17	79.17	N/A	29.93	31.47	29.93	11.97	26.46	26.42	18.51	18.69	18.51
BullGuard	51.72	5.20	1820.96	5.20	13.61	676.62	13.61	26.48	861.16	58.47	88.68	519.99	88.68
Central Command	136.55	5.04	5.44	3.45	14.10	14.25	13.61	62.17	137.28	79.94	136.18	141.23	35.97
Clearsight	96.87	3.90	3.88	N/A	17.89	18.01	17.89	30.10	67.66	66.47	33.74	34.46	33.74
CommTouch	111.91	6.95	6.86	6.95	19.02	18.76	19.02	32.50	71.76	71.76	45.94	46.13	46.50
Defenx	72.94	2.70	14.61	2.70	14.75	180.43	14.75	18.22	338.31	40.22	26.30	293.32	26.30
Digital Defender	78.83	3.86	3.84	N/A	18.09	18.39	18.09	30.42	69.39	67.18	39.72	40.85	39.72
eEye	51.26	1.40	1.40	N/A	6.26	5.02	42.38	20.14	42.86	42.38	32.31	34.25	32.31
Emsisoft	157.82	13.39	13.10	N/A	38.27	41.09	38.27	69.75	155.29	154.02	152.52	163.42	152.52
eScan	142.88	10.90	195.11	10.90	31.89	32.27	31.89	46.88	91.52	103.52	86.66	76.26	86.66
Eset	147.90	5.32	5.35	5.32	17.30	17.62	17.30	95.33	242.88	210.50	54.47	55.00	54.47
ESTsoft	121.24	82.77	260.14	N/A	110.79	215.28	110.79	36.20	300.71	79.94	88.68	238.32	88.68
Fortinet	76.94	8.09	10.29	8.09	12.53	12.67	12.53	31.43	68.64	69.39	33.16	35.20	33.16
Frisk	140.62	10.35	10.41	10.35	24.10	24.26	24.10	39.17	88.94	86.51	97.77	96.94	97.77
G Data	174.71	4.96	1366.06	4.96	23.39	1578.72	23.39	21.66	2104.96	47.84	40.57	1906.56	28.89
GFI	55.57	62.79	67.44	62.79	20.11	19.71	20.11	9.20	20.15	20.31	24.76	24.76	24.76
Hauri	68.16	7.11	6.77	7.11	20.98	21.12	20.98	11.13	24.57	24.57	15.56	15.56	15.56
Ikarus	83.52	5.16	5.16	5.16	13.13	13.18	13.13	29.79	66.01	65.78	60.53	59.89	60.53
Kaspersky	128.23	5.44	7.48	5.44	10.47	16.10	10.47	69.75	177.06	154.02	1.52	1.50	1.52
Microsoft	100.27	4.15	4.03	4.15	18.85	18.70	18.85	44.68	96.66	98.67	34.35	33.94	34.35
Norman	69.70	1.39	1.40	N/A	11.50	11.62	11.50	21.03	48.33	46.43	41.90	42.37	41.90
Preventon	80.02	3.83	3.84	N/A	18.04	18.29	18.04	30.42	69.91	67.18	41.00	41.15	41.00
Quick Heal	226.67	4.23	4.31	4.23	107.03	118.40	107.03	66.51	157.87	161.92	112.15	121.70	86.66
Roboscan	116.47	55.18	273.17	N/A	45.43	485.76	45.43	41.45	574.08	91.52	105.92	279.02	105.92
Sophos	98.66	2.65	2.65	2.65	17.89	17.86	17.89	52.00	119.15	114.82	65.74	42.21	42.37
SPAMfighter	75.92	3.35	3.36	N/A	13.52	13.78	13.52	32.50	73.72	71.76	38.52	39.58	38.52
Symantec	203.09	4.37	455.24	3.69	23.39	182.16	23.39	26.98	228.25	83.09	64.63	134.58	79.44
Tencent	59.58	10.29	10.29	10.29	40.48	45.87	40.48	60.85	133.41	134.36	152.52	156.71	152.52
Total Defense	150.97	182.10	910.48	4.01	70.17	1114.52	71.76	75.26	1262.98	180.43	100.35	672.98	48.27
TrustPort	87.26	4.62	4.65	4.62	20.57	15.75	20.57	33.64	79.27	74.29	37.75	39.31	37.75
UtilTool	86.69	3.91	3.92	N/A	13.79	13.93	13.79	36.20	82.37	79.94	41.45	42.21	41.45
VirusBuster	136.78	4.84	5.28	4.06	14.82	15.50	15.00	40.85	93.79	49.34	123.00	127.10	123.00

* System drive size measured before product installation.

Please refer to text for full product names.





Based, if nothing else, on the false positives clearly recorded in the initial set of logs, no VB100 award can be granted to *Bkis* this month. This is the company's first appearance for a while, but it now has two fails and three passes in the last two years. There were clearly some odd issues here, which must mark the product down to no more than a 'stable' rating.

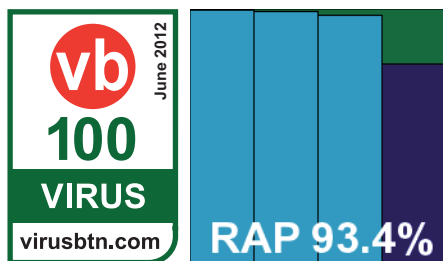
BullGuard Antivirus

Product version: 12.0.218
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

The first of a raft of products this month based on the popular *Bitdefender* engine, *BullGuard* is a fairly regular participant



in our tests with a strong performance record. The current product was submitted as a 146MB package including updates, and again only required a couple of clicks to get going, zipping through in under a minute with no need to reboot. Updates were generally speedy and reliable, although on one occasion a run failed with a message stating that the update server had disconnected unexpectedly. Fortunately, a retry proved more successful, and even with this extra time updates averaged under two minutes.

The product interface bucks the standard approach somewhat, opting for a largely empty GUI dominated by a reassuring 'Your computer is safe' message, with just a few small links and buttons around the outside. With a little exploring, a fair degree of control can be accessed without undue difficulty.

Scanning speeds started off fairly sluggish in most areas, but in the warm runs it blasted through at an incredible pace. On-access overheads were likewise extremely light after an initial settling-in period. RAM use was low, but CPU use a little on the high side, with a fair impact on our set of tasks.

Detection rates, as expected, were stellar, with very little missed in the RAP sets and the Response sets very well covered too. With no issues in the WildList or clean sets,

BullGuard easily makes the grade for VB100 certification, putting the vendor on five passes from five entries in the last six tests; eight from eight in the last two years. The product earns an effortless 'solid' rating.

Central Command Vexira Antivirus

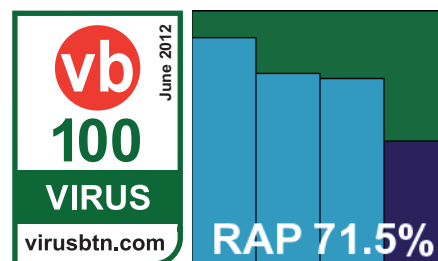
Product version: 7.3.33

Update versions: 5.5.0/14.2.32, 5.5.1/15.0.46, 15.0.51, 15.0.53

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

False positives 0

Central Command's Vexira has settled in as a firm regular which rarely misses a test these days, and generally puts in a decent



showing. The underlying engine is from *VirusBuster*, and as usual for server tests, a full-blown server solution was provided. The installer was relatively compact at 69MB, with 92MB of updates also required for the offline parts of the test. Set-up was fairly straightforward, following through a standard selection of 10 or so steps. As noted in previous tests, the option to send feedback on detections and so on to the developers is rather deviously concealed on the EULA screen where one would usually expect a checkbox to accept the terms and conditions. While we would usually encourage people to participate in these schemes, some server admins (used to handling highly sensitive information) may find this approach more than a little sneaky. Assuming one is not required to be extra paranoid and read through each page in minute detail, the set-up process takes less than a minute, with a reboot required at the end. Once up and running, updates can be initiated manually, but on each of the five or six installs needed to complete testing, this first attempt failed with no information as to why. Leaving it alone for five minutes or so seemed to do the trick though, with a message saying it had at last managed to complete the required download of data.

The interface is another MMC-based monster, which manages to pull off the trick of making the console system even more awkward, fiddly, unintuitive and inconsistent than it needs to be. A decent level of controls is provided, but they must be wrestled out of what is at times a

bewildering layout. As always with this product and its *VirusBuster* sister solution, an option to scan archives internally on access appears to be provided, but has no effect whatsoever.

Scanning speeds were sluggish in the archive and binary sets but pretty nippy in other areas, especially with the default settings where file extensions are trusted as a guide to file content. On-access overheads showed a similar pattern, with much time spent looking at some sets while others were mainly ignored. Memory consumption was fairly low, and CPU use not too high either, with a reasonable hit on our set of tasks.

Detection rates were not stellar, but not too disappointing either, with decent coverage of the reactive parts of the RAP sets, dropping off sharply into the proactive week, and a reasonable showing elsewhere. The WildList sets were well handled, and with no issues in the clean sets a VB100 award is earned. With a single hiccup a few tests back, *Vexira* boasts five passes and a single fail in the last six tests; 11 passes in the last two years. This month the product earns a ‘solid’ rating for stability.

Clearsight Antivirus

Product version: 2.1.89

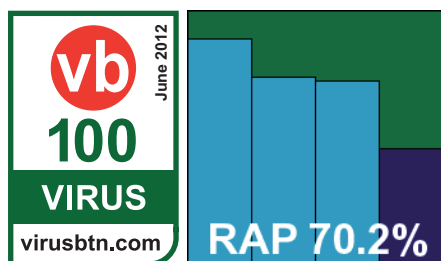
Update versions: 14.2.31, 15.0.46, 15.0.51, 15.0.53

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

ItW Extd 100.00% ItW Extd (o/a) 99.86%

False positives 0

The last comparative saw something of a glut of solutions from the same white-label factory, using the *VirusBuster* engine with a



front end provided by *Preventon*; this month only a handful returned – most of them, including this one, among a small group of long-term semi-regulars. *Clearsight*’s version came as a 90MB installer, which ran through in a small number of steps, completing in just half a minute or so with no need to reboot. The interface is simple and basic, with a slightly more than minimal set of controls, but is generally easy to operate and responsive. On this occasion we observed a couple of interface crashes, both of which appeared when the licence code was entered shortly after installation – but this didn’t seem to cause any lasting

effects and simply reopening it got things moving again. There were a few other oddities with the interface that we had not previously observed, such as slots of scan times and numbers of files scanned sitting empty in the scan dialog. Previously mentioned problems, such as the right-click scan ignoring options not to remove or quarantine detected items, remained present.

Scanning speeds were fairly mediocre, but overheads weren’t too heavy and memory use was low. CPU use was a little on the high side, but our set of tasks ran through in good time. Detection rates were a little below par but not terrible (as expected having seen several performances from the same engine so far), with acceptable rates in the Response sets. RAP scores were initially baffling, seeming reasonable in the reactive parts but terrible in the proactive week. Further investigation showed the scan had silently given up on encountering a tricky packed file in the set. Removal of this and several similar items gave us a more complete picture, which was much closer to our expectations, but still showed a fairly steep decline. The WildList sets were handled without any problems though, and with nothing to trouble us in the clean sets a VB100 award is duly granted. With a few stability issues noted, *Clearsight* is rated no more than ‘fair’ in our new system, but has five passes from five entries in the last six tests; seven from seven in the last two years.

CommTouch Command Anti-Malware

Product version: 5.1.16

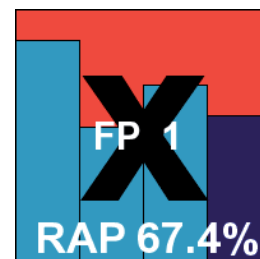
Update versions: 5.3.14/201204190953, 201206061023, 201206081258, 201206120807

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

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

False positives 1

Another product based on a third-party engine, although with rather more additional protection rolled in, *CommTouch* has had a rather rocky time in our tests of late. This month’s offering was as compact as ever, with the main package only 14MB and offline updates just 28MB. The set-up process is fairly simple and speedy, needing no reboot, and updating online was pleasingly fast too, taking no more than four minutes to complete the whole install.



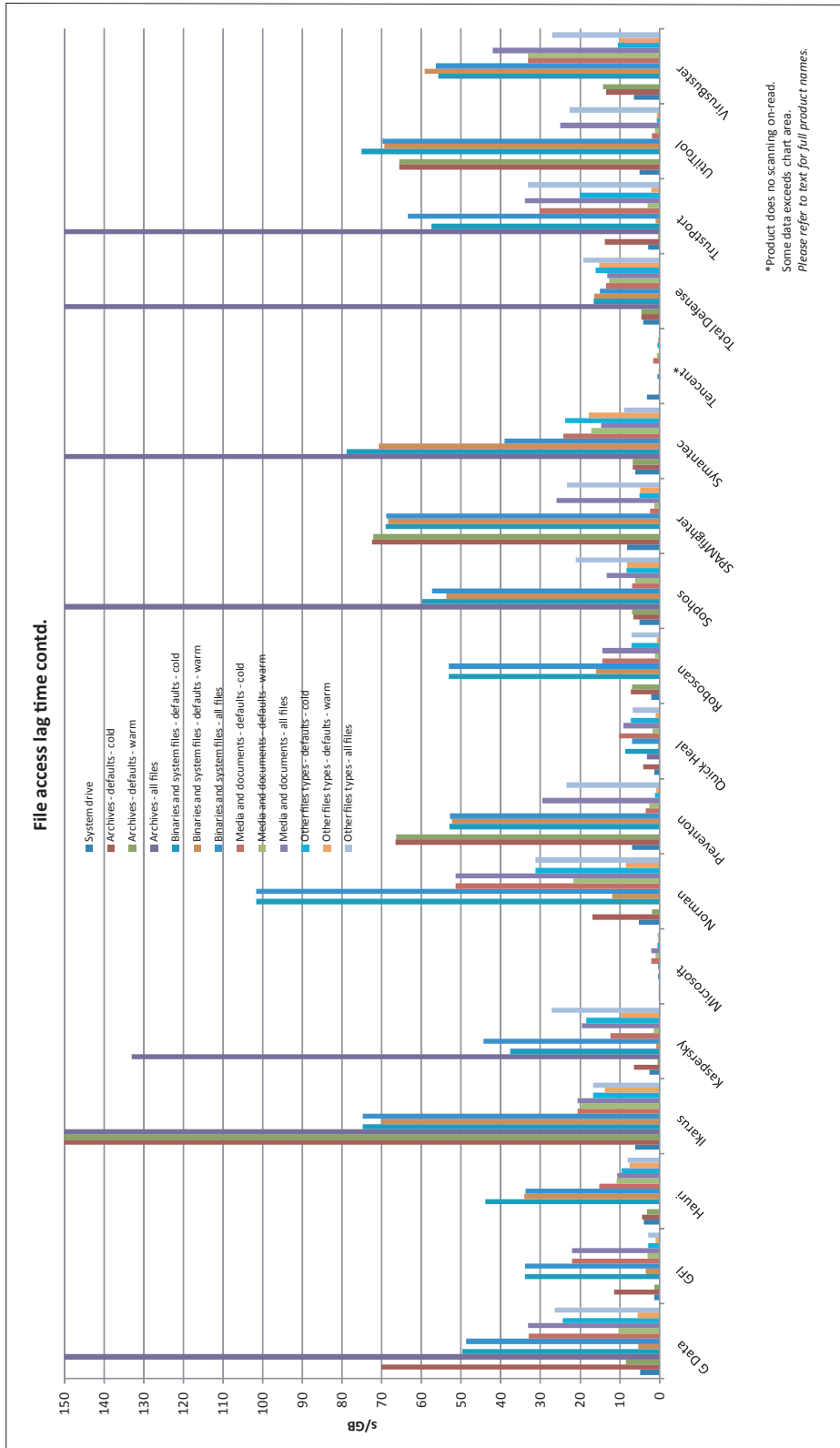
The interface is fairly basic, but has a reasonable set of controls, and seemed pretty sturdy under pressure. Scanning

File access lag time (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum	1.60	22.96	0.72	N/A	40.46	0.74	40.46	47.05	1.44	47.05	47.44	1.04	47.44
Avast	1.36	11.37	7.23	125.80	17.17	16.10	39.08	1.88	0.95	16.90	0.57	0.44	16.44
AVG	3.07	2.94	0.61	N/A	26.88	0.89	3.26	10.30	0.71	6.83	3.91	0.31	8.43
Avira	3.60	7.02	4.44	45.31	26.58	12.34	26.61	36.73	25.19	37.63	14.17	14.05	13.94
Bitdefender	2.76	154.46	0.04	155.39	44.53	14.91	39.08	15.61	0.13	14.73	8.83	0.30	8.93
Bkis	7.55	7.72	7.84	N/A	21.14	21.42	21.14	49.43	47.57	49.43	30.89	30.68	30.89
BullGuard	3.63	187.60	12.74	N/A	43.60	17.89	43.60	20.29	3.19	20.29	11.22	2.61	11.22
Central Command	5.08	11.70	0.30	1.12	69.70	49.57	49.39	12.80	11.84	21.40	2.81	3.08	20.07
Clearsight	5.09	66.36	66.17	N/A	52.54	52.20	53.21	4.01	3.11	31.26	1.30	1.14	27.99
CommTouch	7.01	156.94	175.42	174.91	74.67	67.34	66.40	56.09	54.60	54.08	17.68	16.79	16.45
Defenx	3.08	21.94	2.38	N/A	50.96	12.07	50.96	81.43	22.14	81.43	52.41	8.55	52.41
Digital Defender	6.94	68.09	67.52	N/A	52.81	52.25	51.97	3.48	2.47	29.91	1.09	0.88	23.75
eEye	12.48	17.88	17.92	N/A	112.87	112.51	112.87	52.86	52.97	52.86	32.07	31.65	32.07
Emsisoft	1.10	6.90	6.72	N/A	19.31	16.83	125.32	1.58	0.62	110.21	0.27	0.22	71.51
eScan	1.45	7.78	0.06	12.58	43.07	14.93	32.63	19.51	0.13	24.19	10.52	0.37	18.95
Eset	1.01	1.02	0.89	N/A	5.87	5.67	5.42	4.55	3.70	3.06	2.22	2.08	1.62
ESTsoft	1.51	8.52	0.16	N/A	36.72	0.34	36.72	13.70	1.04	13.70	7.24	0.64	7.24
Fortinet	8.49	73.38	0.24	73.38	53.69	0.27	53.69	11.26	0.92	11.26	18.55	0.69	18.55
Frisk	3.56	10.68	11.23	N/A	38.52	37.59	38.52	8.69	7.76	8.69	6.75	6.47	6.75
G Data	4.80	70.07	8.38	281.55	49.69	5.29	48.75	32.93	10.38	33.07	24.38	5.55	26.41
GFI	1.36	11.36	1.35	N/A	33.92	3.42	33.92	22.00	2.94	22.00	2.85	0.98	2.85
Hauri	3.97	4.42	3.11	N/A	43.94	33.99	33.81	15.23	10.85	10.62	9.55	7.50	8.03
Ikarus	6.15	188.04	188.42	188.04	74.87	69.92	74.87	20.57	19.65	20.57	16.76	13.77	16.76
Kaspersky	2.59	6.48	0.56	132.99	37.60	0.87	44.35	12.32	1.48	19.55	18.47	9.63	27.21
Microsoft	0.10	0.09	0.03	N/A	0.34	0.06	0.34	2.01	1.04	2.01	0.53	0.37	0.53
Norman	5.20	16.85	1.93	N/A	101.69	11.83	101.69	51.45	21.73	51.45	31.29	8.49	31.29
Preventon	6.93	66.55	66.33	N/A	52.98	52.32	52.85	3.40	2.51	29.56	1.07	0.88	23.48
Quick Heal	1.21	4.03	0.13	3.15	8.63	0.37	6.97	10.21	1.78	9.10	7.20	0.95	6.80
RoboScan	2.05	7.27	6.83	N/A	53.12	15.97	53.12	14.33	1.10	14.33	7.00	0.60	7.00
Sophos	4.99	6.64	6.85	352.71	59.79	53.69	57.37	6.95	6.06	13.24	8.25	8.13	21.03
SPAMfighter	8.07	72.50	72.16	N/A	69.04	68.36	68.86	2.43	1.34	25.92	5.01	4.94	23.34
Symantec	6.10	6.76	6.70	155.39	78.80	70.69	39.08	24.28	17.27	14.73	23.69	17.84	8.93
Tencent	3.15	0.20	0.13	N/A	0.49	0.26	N/A	1.64	0.71	N/A	0.53	0.38	N/A
Total Defense	4.11	4.59	4.61	171.94	16.63	16.38	14.96	13.49	12.74	13.10	16.09	15.22	19.28
TrustPort	2.82	13.81	0.28	335.27	57.45	0.95	63.34	30.08	3.03	33.86	19.93	2.02	33.07
UtilTool	5.09	65.62	65.62	N/A	75.06	69.27	69.87	1.88	1.10	25.04	0.70	0.62	22.63
VirusBuster	6.36	13.40	14.16	N/A	55.71	59.23	56.40	33.15	33.17	41.95	10.43	10.24	27.08

* System drive size measured before product installation.

Please refer to text for full product names.





speeds were reasonable, but overheads were decidedly heavy with the on-access measures taking quite some time to complete. Although RAM use was low, CPU use was very high and our set of activities also took a very long time to get through.

Detection rates were not great – a little unpredictable through the RAP sets and not too impressive through the Response sets either, but the WildList at least was well handled. In the clean sets, a single item – apparently a fairly old and packed installer for some drivers provided with some much newer hardware – was alerted on with a heuristic flag, which was enough to deny *Commtouch* a VB100 award this month. That leaves the vendor looking rather wobbly, with two passes and three fails in the last six tests; four passes and five fails from nine entries in the last two years. Stability this month was fine though, earning the product a ‘solid’ rating.

Defenx Security Suite 2012

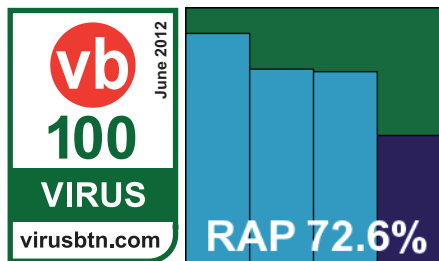
Product version: 3735.575.1669

Update versions: 19/04/2012, 07/06/2012, 11/06/2012, 13/06/2012

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

False positives 0

Sticking with an OEM theme, malware detection in the *Defenx* product is provided by *VirusBuster* by way of *Agnitum*, whose suite this



strongly resembles. The 127MB installer needs only a couple of clicks but takes a while to complete, including updating and gathering ‘smart scan data’, with a reboot required at the end; the whole process takes around five minutes.

The interface is clear and well laid out, with good access to a decent level of controls, and we generally found that it responded well. At one point, after running an intense on-access job with multiple infections, we had some problems opening *Notepad* or *WordPad* to peruse plain-text logs. Many other functions were also unavailable, as if the high number of detections in such a short time had put the system into some sort of lockdown mode. After ten minutes or so this seemed to clear though, and the usability was restored.

Scanning speeds were not super-fast initially, but they improved greatly in the warm runs, while file access lag times were a little high in the archive and binary sets, but very low elsewhere. RAM use was unexceptional, but CPU use was pretty high, with a heavy impact on our set of tasks. Detection rates were much as expected: decent in the early parts of the RAP sets with a steep decline into the proactive week, reasonable in the Response sets, with no issues in the core certification sets. A VB100 award was earned without complaint. Some oddities observed after heavy bombardment rule out a perfect score for stability, but they don’t drag it too far down the rankings, leaving it on ‘stable’. Our test history shows ten passes from ten entries in the last two years, only the annual *Linux* tests not entered.

Digital Defender AntiVirus for Servers

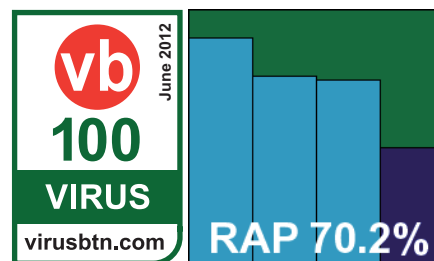
Product version: 2.1.89

Update versions: 14.2.31, 15.0.46, 15.0.51, 15.0.53

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.86%

False positives 0

Another product from the *Preventon!* *VirusBuster* stable, with a fairly long and respectable history in our tests, *Digital Defender’s*



latest edition was submitted as an 88MB install package, which ran through quickly and simply with no reboot needed. The by now very familiar interface provides basic controls but is clearly and simply laid out, generally responding well under pressure. A few minor bugs were noted, but there were no serious issues or crashes until the latter stages of the RAP sets, where once again scans simply aborted with no alert or warning, and some files had to be removed before they could be coaxed through to the end.

Scanning speeds elsewhere were not bad, with overheads a little above average in some areas but very light in others; resource use and impact on our set of tasks were reasonable too. Detection rates held no surprises, dropping sharply through the RAP sets from a decent starting point. Response scores were mostly decent too, and with no issues in the WildList or clean sets a VB100 award is earned. That gives *Digital Defender* five passes from five entries in the last six tests; seven passes and three fails in the last two years, and a ‘stable’ rating.

eEye Blink Server

Product version: 5.0.2

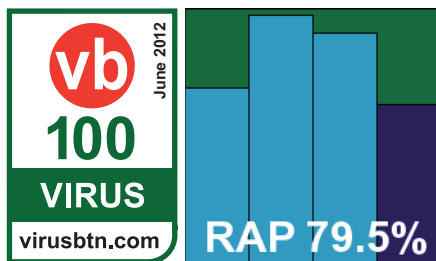
Update versions: 1.1.2084, 1.1.2157, 1.1.2159, 1.1.2160

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

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

False positives 0

Not long after receiving the submission for this month's test, we received word that *eEye Digital Security* had been acquired



by *BeyondTrust*, so it seems likely that in future reports we will no longer see the *eEye* name. The product has put in a run of good showings of late. Malware detection mainly stems from the *Norman* engine incorporated in the product, including its *Sandbox* analysis system.

The installer submitted this month was a fair size, at 231MB, but it didn't take too much effort to run through, completing in not much over a minute with no reboot required and a short set-up wizard at the end. Online updates weighed in at a hefty 200MB, but generally took no more than a couple of minutes to fetch.

The interface focuses mainly on the vulnerability management which is the product's main strength, but reasonable space is given to the anti-malware configuration, with a decent basic level of controls. Scanning speeds were very slow over archives and binaries, but perfectly reasonable elsewhere; overheads were pretty hefty throughout the sets, although our set of tasks didn't take too long to get through, with average RAM use and fairly high CPU consumption.

Detection rates were pretty decent in the Response sets; RAP tests were hindered by scans repeatedly snagging on a particular cluster of samples (the product sitting on one for an entire weekend), and even with dozens removed we were only able to get partial results for the oldest week of samples. This threw the scores out a little, but we would extrapolate those we did record to give pretty decent reactive rates, with the proactive week showing a fair decline. The core sets were handled well, and a VB100 award is easily earned. The only issues noted were with specific malicious files and would be unlikely to upset any real-world users, nevertheless a not-quite-perfect 'stable' rating is all that can be granted. Our test history shows a

decent record of late, with four passes and one fail from five entries in the last six tests; seven passes and two fails in the last two years.

Emsisoft Anti-Malware

Product version: 6.5.0.11

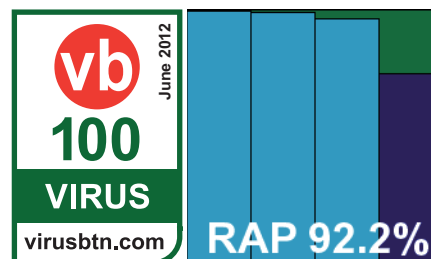
Update versions: N/A

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

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

False positives 0

Emsisoft has been battling some bad luck with false positives in our tests for a while now, and comes into this comparative hoping for a



change of fortunes. The current version measured 128MB, and installed with just a couple of clicks; the interface is a little quirky and unusual, but is reasonably easy to navigate, providing a decent basic level of controls.

Speeds were very quick on demand, with generally very light overheads on access, although much of this may be down to the default behaviour of not checking much on-read; with more thorough settings similar to most other products, speeds decreased considerably. Our set of tasks still took some time to complete, but resource use was on the low side.

Detection rates were as excellent as we have come to expect from this product and the *Ikarus* engine included in it, with very impressive RAP and Response scores. With no issues in the WildList, a clean sheet in the false positive sets was enough to break *Emsisoft's* run of misfortune, earning the product its first VB100 award for a while. This is the product's first pass from five entries in the last six tests; longer term, we see three passes from nine entries. Stability was 'solid'.

eScan Internet Security Suite

Product version: 11.0.1139.1184

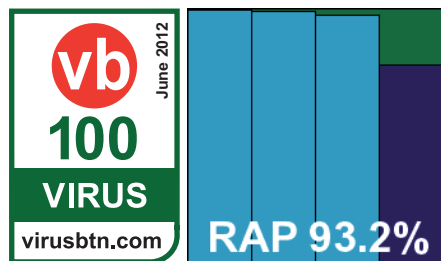
Update versions: N/A

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

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

False positives 0

Sticking with third-party engines, *eScan* is another *Bitdefender*-based solution, although like the previous entry it includes much



of its own input. The installer was towards the upper end of the scale at 180MB. It ran through in a number of stages with moments of action interspersed with further queries, completing with a speedy scan and a request for a reboot. Updates were a little on the slow side, averaging just over five minutes over all the runs.

The interface is fairly flashy and stylish, but is also simple to operate, providing an excellent degree of fine-tuning in a much more sensible fashion underneath the glitzy exterior. Scanning speeds were pretty good, and overheads pretty light, with low use of memory, average CPU use and a minimal effect on our set of activities. Scores were as excellent as expected in the RAP sets, but strangely disappointing in the Response sets, hinting that updating had not run as smoothly as we had been led to believe. Nevertheless, the core sets were properly dealt with, and a VB100 award is duly earned. The vendor's recent history is very good, with six passes out of six this year; ten passes and two fails in the last two years. The product's stability this month was rated 'solid'.

Eset NOD32 Antivirus 4

Product version: 4.2.76.0

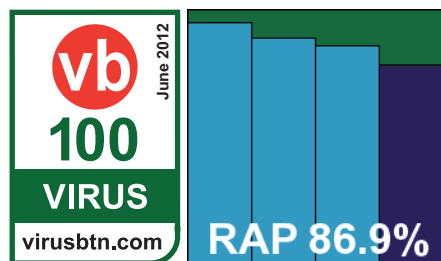
Update versions: 7067, 7200, 7206, 7215

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

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

False positives 0

Finally we come to a product including no third-party engine. *Eset* came into this comparative looking to maintain a



record-breaking streak of successful appearances. The current product came in as a fairly lightweight 56MB installer, which ran through a very familiar set of steps,

including the trademark insistence on explicitly choosing whether or not to alert on 'potentially unwanted' items. The process completed in good time with no reboot required; updates were likewise zippy to the point of being unnoticeable.

The interface is familiar from long exposure over the last few years, looking good and providing splendidly complete configuration with decent clarity of layout. A few places still seem to overlap somewhat perhaps, and we continue to question whether we are using the on-access archive unpacking controls incorrectly, or whether they simply don't work.

Testing tripped along nicely, with solid speeds on demand and incredibly light overheads on access. RAM use was lowish and CPU use not bad either, and our set of activities zipped through in splendid time. Detection rates were solid, with a good showing in the Response sets and strong scores in the RAP tests – a little behind the leaders in the reactive weeks but well up with the pace in the proactive week. The core sets were once again handled without issues, although a number of suspicious alerts were recorded in the clean sets, most of them quite accurately highlighting toolbars and other extras of dubious merit. *Eset* thus comfortably earns a VB100 award, extending its epic unbroken run still further – the product has 12 passes in the last two years. With no problems of note, *Eset* earns a 'solid' stability rating.

ESTsoft ALYac Enterprise

Product version: 2.5.0.18

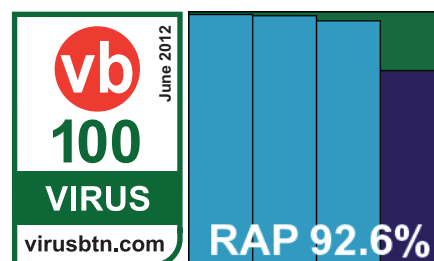
Update versions: 12.3.20.1/425083.2012041810/7.4193
3/7073173.20120417, 425498.2012041913/7.41962/707
7818.20120419

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

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

False positives 0

Returning after having some serious problems last time around, *ALYac* is another product based on the increasingly popular



Bitdefender engine, again with some extra stuff in the form of the Korean company's own '*Tera*' engine. The installer submitted was 141MB, and the set-up process was fairly straightforward, following the standard pattern of stages,

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum	OD	X	√	√	√	X	X	√	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Avast	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
AVG	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Bitdefender	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	4/√	4/√	8/√	X/√	X/√	X/√	X/√	X/√	X/√
Bkis	OD	X	X	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
BullGuard	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	2	2	1	1	2	2	2	1	2	2	√
Central Command	OD	X	√	√	√	X	√	√	√	√	X/√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Clearsight	OD	2	2	X	X	2	X	2	2	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Commtouch	OD	5	5	5	5	5	√	5	5	5	5	√
	OA	2/4	2/4	2/4	2/4	2/4	√	2/4	1/2	2/4	2/4	√
Defenx	OD	X	√	√	√	√	X	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Digital Defender	OD	2	2	X	X	2	X	2	2	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√

Key:

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

X - No detection of EICAR test file

X/√ - Default settings/all files

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

* Detection of EICAR test file with randomly chosen file extension

** No apparent detection of EICAR test file on access

Please refer to text for full product names.

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
eEye	OD	X	1	1	1	1	1	1	8	1	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Emsisoft	OD	2	2	X	X	2	2	2	3	2	2	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
eScan	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	1/√	X/√	X/√	X/√	X/√	√
Eset	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ESTsoft	OD	X	X	8	8	X	X	X	X	X	X	√
	OA	X	X	8	8	X	X	X	X	X	X	√
Fortinet	OD	2	√	√	√	√	√	√	√	√	√	√
	OA	2	√	√	√	√	√	√	√	√	√	√
Frisk	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	2	2	X	X	X	X	2	2	√
G Data	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	8/√	8/√	√	√
GFI	OD	X	X	√	√	√	X	√	X	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Hauri	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Ikarus	OD	7	7	7	7	7	7	7	3	7	7	√
	OA	7	7	7	7	7	7	7	3	7	7	√
Kaspersky	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	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

** No apparent detection of EICAR test file on access

Please refer to text for full product names.

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Microsoft	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	X	1	X	X	X	1	X	√
Norman	OD	X	√	8	1	√	√	√	8	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Preventon	OD	2	2	X	X	2	X	2	2	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Quick Heal	OD	X/1	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	OD	X	X	8	8	X	X	X	X	X	X	√
	OA	X	X	8	8	X	X	X	X	X	X	√
Sophos	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
SPAMfighter	OD	2	2	X	X	2	X	2	2	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Symantec	OD	3/√	3/√	3/√	3/√	3/√	3/√	3/√	3/√	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Tencent	OD	√	√	√	√	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	X**
Total Defense	OD	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
TrustPort	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	√	X	X	X	1	1	√
UtilTool	OD	2	2	X	X	2	X	2	2	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
VirusBuster	OD	X/2	X/√	X/√	X/√	X/√	X	X/√	X/√	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

** No apparent detection of EICAR test file on access

Please refer to text for full product names.

taking about a minute to get through and needing a reboot at the end. Running updates once again seemed unreliable, with several attempts taking several minutes before baling out. Once again, the only way of telling this had happened was an error message which disappeared after five seconds – users not monitoring the process closely as it fetched several hundred files would easily have missed this and would have been presented only with the misleading information that an update attempt had been run. Eventually we seemed to get a complete job finished satisfactorily on each install, or so it appeared.

The product interface is fairly attractive and reasonably well laid out, although a few oddities of translation make some sections less than lucid. Configuration is fairly rudimentary but the basics are available, and after some serious issues in the last comparative, stability this time was much improved.

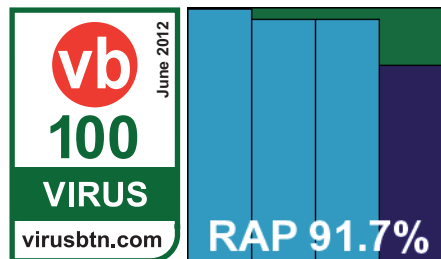
Speeds were superb on demand, with on-access overheads pretty light; resource use was around normal, with an average impact on our set of activities. Detection rates were stunning in the RAP sets, as expected, but once again we saw a significant drop in the Response sets, implying that updating may not have been as successful as we had been led to believe. The core sets were properly dealt with though, and a VB100 award is duly earned. Officially *ESTsoft* now has three passes from three entries in its first year of participation, but an entry in the last test was not included due to there being too many problems in getting it to work. Some suspect updating behaviour this month has apparently now been addressed by the developers, but still marks the product down to only ‘fair’.

Fortinet FortiClient

Product version: 4.1.3.146
 Update versions: 4.3.396/15.439, 4.3.398/15.650, 15.655, 15.677

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

Fortinet has shown some impressive improvements of late, with scores rapidly catching up with those of its rivals apparently mainly due to heuristic rules being improved and turned



up. The current product came as a very small 10MB main package with 33MB of updates, and set up in less than half a minute with just the standard set of stages to click through. No reboots were needed, and updates took only a couple of minutes extra to get done.

The interface is unflashy and businesslike, providing a decent degree of fine-tuning, but the default settings are pretty thorough and there was little we needed to adjust. Scanning speeds were not the fastest, and overheads were perhaps a fraction on the high side in some parts of the sets, and while resource use was not exceptional, our set of activities took rather a long time to complete.

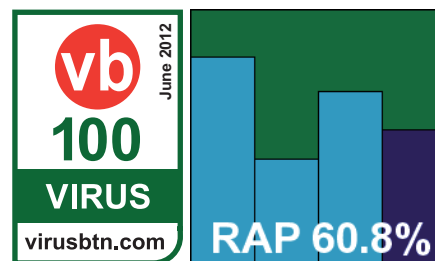
Detection rates were good though, well up with the leading pack on the RAP chart and with a strong showing in the Response sets too. No issues were encountered in the core sets, and a VB100 award is thus earned without fuss. *Fortinet's* test history now shows five passes from five entries in the last six tests; nine from ten in the last two years. The product earns a ‘solid’ stability rating this month.

Frisk F-PROT Antivirus for Windows

Product version: 6.0.96
 Update versions: 4.6.5

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

Frisk's product is one of the least changed in the last several years, and the latest version brought no surprises. The installer weighed in at 25MB, with 27MB of updates, and ran through just a handful of steps, taking less than half a minute to complete but needing a reboot at the end. The interface remains bleak and chilly, but with a certain charm to its simplicity. It provides only basic configuration, and it seemed mostly stable and responsive through the tests.



Scanning speeds were decent, and overheads fairly light, with low use of RAM but pretty high CPU consumption; our set of tasks ran very quickly indeed though, barely distinguishable from the baseline measures. Detection rates were less splendid however, coming in towards the bottom of the pile in both the RAP and Response sets, the RAP scores once again showing a bewildering refusal to conform

to the expected patterns. The core sets were properly handled though, and *Frisk* earns a VB100 award. With stability rated as 'solid', our test history for *Frisk* also looks good, with all of the last six tests passed; ten passes and two fails in the last two years.

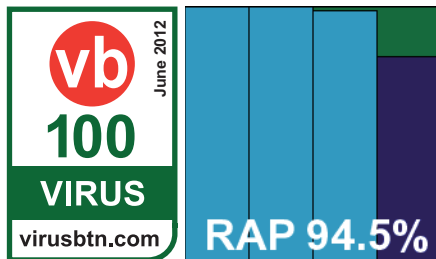
G Data AntiVirus Administrator/Client

Product version: 11.5.2.133
 Update versions: AVA 22.4657/AVL 22.857, AVA 22.5203/AVL 22.969, AVA 22.5256/AVL 22.974, AVA 22.5280/AVL 22.974

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

False positives 0

Another proper server-oriented product, this one came in as a monster 636MB executable. This turned out to be a full-blown



management server administration utility which took some work to install, first attempts failing thanks to not having the .NET framework ready to go on the test systems. With the .NET framework in place, the process was re-run, and turned out to be reasonably simple, including the set-up of an *MS SQL* database system among many other tasks. No initial reboot was requested, but we later discovered that restarting the machine made things work much more smoothly. With the administrator set-up, we then deployed the client component to the local system. On about half of the installations performed, this was a simple process, with the local system immediately offered as a potential target, but on the other half the list of available targets was empty and the machine had to be specified by name; in these cases a reboot was also needed to enable the client to deploy. Once this stage was complete, the actual installation took place on a seemingly arbitrary schedule, and the machine had to be left alone for a while until it happened. On some occasions a reboot was needed to get the client interface available, while on others it materialized in the system tray of its own accord.

Configuration is available through the administration interface, including reporting and scheduling of tasks, but we opted to cede control to the client subsystem for simplicity. Updates, however, were performed from the

administration unit, and again it was difficult to predict just how long they would take, both to download to the management system and to deploy to the client. Over all the installations performed, at least half an hour was needed to get from bare system to fully functioning, up-to-date client.

From there on things were much more straightforward, with scanning speeds reasonable from the off and blasting through in the warm runs. Overheads were initially a little heavy, but soon became barely perceptible. As predicted – and warned about by the product itself – turning the thoroughness of scanning up increased the overheads considerably. CPU and RAM use were a little on the high side – likely at least in part due to the administration system being present – and our set of tasks took somewhat longer than average to get through, though not disastrously so.

Detection rates were, as ever, pretty remarkable, with barely anything missed in the reactive part of the RAP sets, and the proactive part well covered too; Response scores were pretty decent. The WildList sets presented no difficulties, and with no false alarms either, another VB100 award goes to *G Data*, putting it on five passes from five entries in the last six tests; eight from ten in the last two years. The product earns a 'stable' rating thanks to the unpredictable deployment experience.

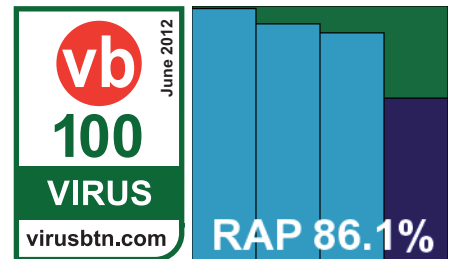
GFI VIPRE Antivirus 2012

Product version: 5.0.5134/5.2.5162
 Update versions: 3.9.2533.2/11809, 3.9.2539.2/12016, 12044, 12049

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

False positives 0

GFI's VIPRE is a relative newcomer on the anti-virus scene, but in a few brief years it has picked up a solid reputation, with a decent



record in our tests. As ever, the main package is very compact at just 11MB, with updates a little larger at around 80MB. The install process is slick and glitzy, with a single licensing screen followed by a quick slideshow boasting of the product's prowess, which completes in under a minute with an offer to join another 'ThreatNet' data-gathering scheme.

The product interface is similarly slick and pretty, but is rather short on configuration for business purposes; the options that are available are at times less than obvious in their intent. With some experience, though, operation is reasonably straightforward – although as usual a combination of initially allowing access to some complex items with delayed scanning implemented and curtailing of logs to the last 100 entries makes the on-access tests a little more trying than some. Awkward and wasteful XML logs for the on-demand scans have also been problematic in previous tests, but the provision of a simple parsing tool has made those worries a thing of the past.

Scanning speeds were decent throughout, and overheads pretty light, with very low use of memory, lowish CPU use and a low impact on our activities. Detection rates were pretty impressive – a little behind the very best this month but keeping pretty close to the pace in the RAP tests, with Response scores similarly impressive. The core sets were correctly dealt with, and with no major issues to report *GFI* earns another VB100 award. A few large scan jobs did fail to complete happily – invariably those dealing with large numbers of detections – so a ‘stable’ rating is the best we can offer this month. Our test history shows four passes from five entries in the last year; eight out of nine in the last two years.

Hauri ViRobot Server Protection 2011

Product version: 6.0.0.0

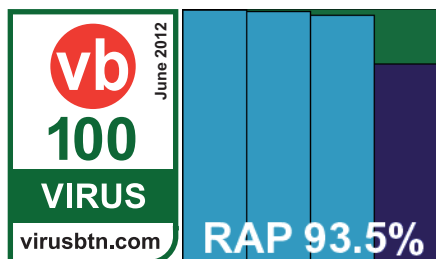
Update versions: N/A

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

False positives 0

Bucking the standard trend which sees 2013 products start to emerge when 2012 is little more than halfway through, *Hauri* sticks to a 2011

branding. With the vendor’s history in our tests sporadic and less than illustrious, we hoped to see some improvement from a product which, based on the popular and usually strong *Bitdefender* engine, should really do very well indeed. The installer provided was a fair size at 167MB, but didn’t take long to run through its business. Updates were a little on the slow side (the company perhaps focusing its



efforts on its home market in Korea), but there didn’t seem to be any problems.

The interface is slick and professional-looking, echoing the black-and-red colour scheme of *Bitdefender*’s own product lines. It favours the large-icon-and-button approach, but a good level of configuration is provided under the covers and it generally responded well. Under pressure we did see the GUI crash out a couple of times, not always when dealing with large amounts of malware.

Speeds on demand were a little underwhelming, but on-access lag times were reasonable; resource use was fairly low and our set of tasks took a little more than most to complete. Detection rates in the RAP sets were excellent, closely mirroring several other products based on the same technology, but again the Response sets showed much lower scores than expected, suggesting yet another issue with updating. The core sets were properly dealt with in spite of this though, and *Hauri* earns a VB100 award – breaking a streak of bad luck that has lasted a couple of years. A few minor crashes were observed, but nothing too severe and only at high-stress times, thus earning the product a ‘stable’ rating. Our test history for *Hauri* now shows one pass along with two fails in the last six tests; one pass from five entries in the last two years.

Ikarus virus.utilities

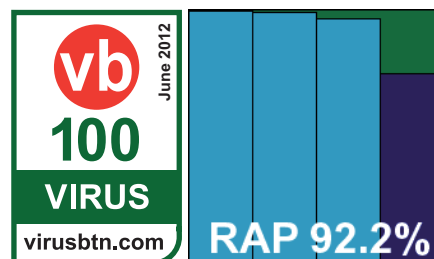
Product version: 2.0.134

Update versions: 1.1.118/80976, 81423, 81454, 81473

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

False positives 0

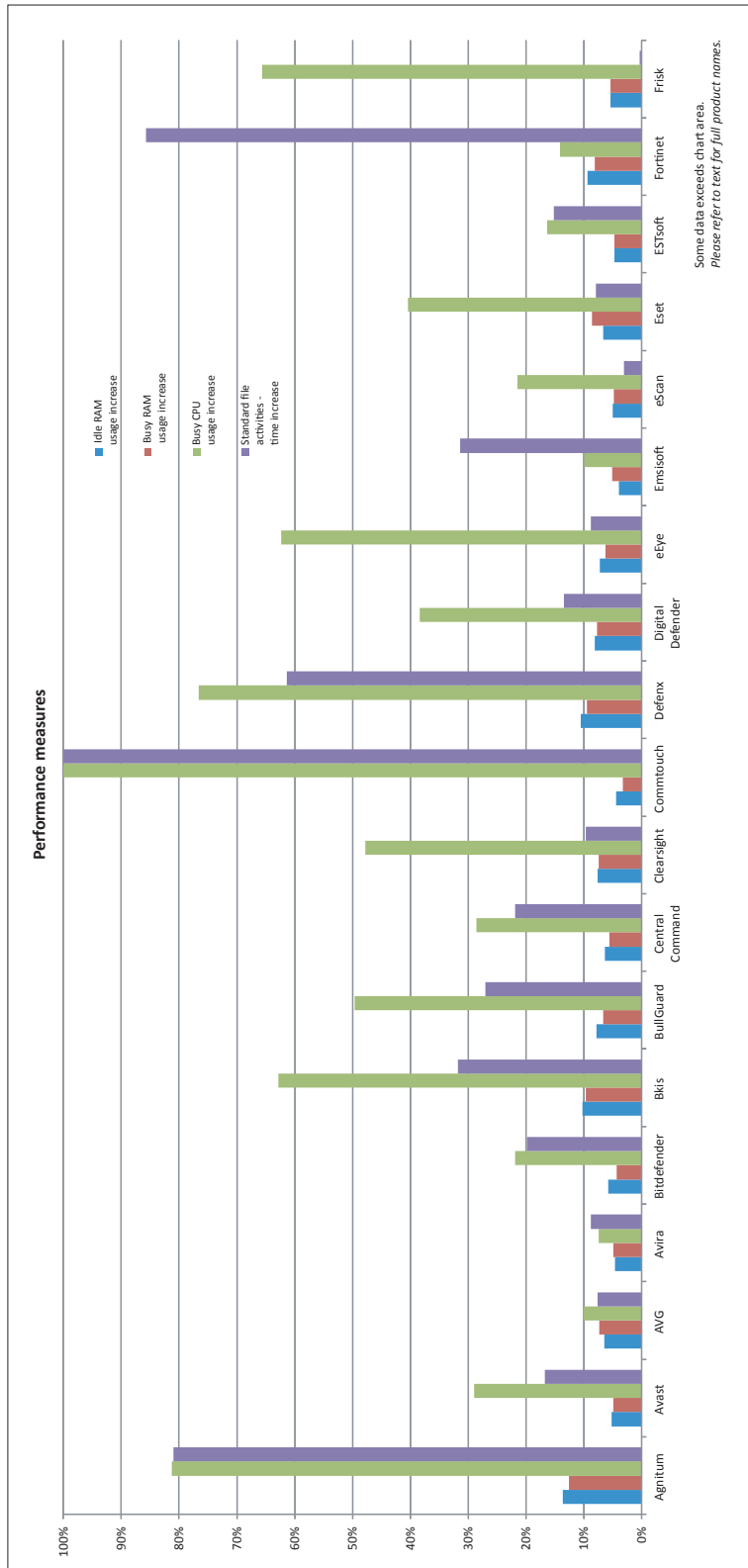
Ikarus is another product that has changed little since we first encountered it several years ago, although we have heard that a change

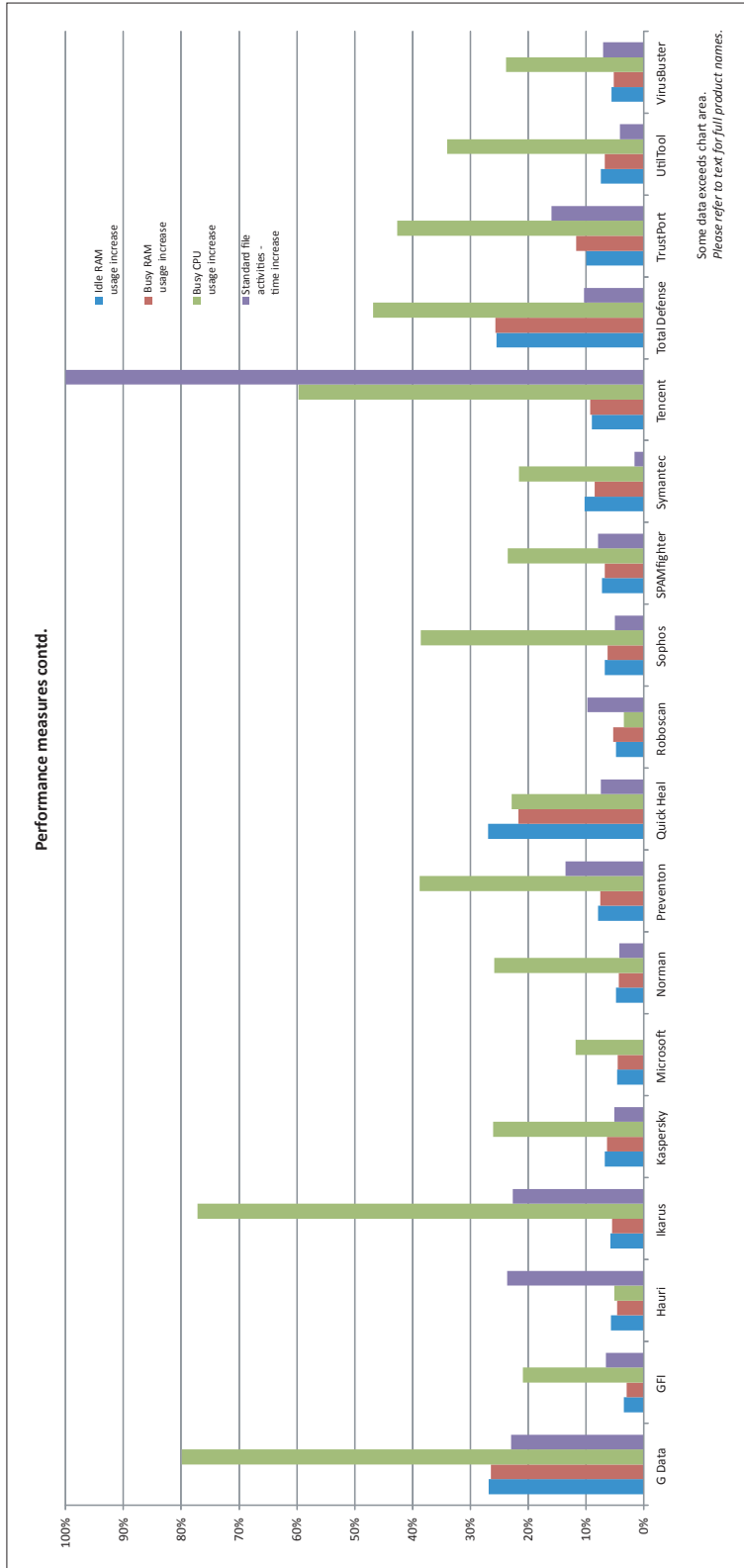


of name is in the offing, and it may well be that a refresh of the interface will accompany it. For now, we stick with a familiar pattern: the product was provided as a complete CD ISO image measuring just over 200MB but containing much more besides the basics, along with updates in a separate 73MB archive. The installation process is pretty simple and speedy, running through a few initial steps then rushing to completion in moments. Online updates took a little longer,

Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities - time increase
Agnitum	13.66%	12.61%	81.30%	80.99%
Avast	5.21%	4.87%	28.94%	16.74%
AVG	6.44%	7.29%	10.04%	7.62%
Avira	4.63%	4.88%	7.40%	8.77%
Bitdefender	5.78%	4.34%	21.88%	19.86%
Bkis	10.20%	9.66%	62.85%	31.74%
BullGuard	7.83%	6.66%	49.59%	27.00%
Central Command	6.38%	5.60%	28.53%	21.83%
Clearsight	7.59%	7.39%	47.81%	9.69%
CommTouch	4.42%	3.21%	100.90%	169.56%
Defenx	10.56%	9.48%	76.59%	61.34%
Digital Defender	8.07%	7.76%	38.34%	13.44%
eEye	7.26%	6.22%	62.36%	8.79%
Emsisoft	3.90%	5.06%	9.93%	31.36%
eScan	4.97%	4.77%	21.51%	3.03%
Eset	6.64%	8.55%	40.40%	7.89%
ESTsoft	4.67%	4.72%	16.37%	15.16%
Fortinet	9.40%	8.10%	14.16%	85.76%
Frisk	5.42%	5.40%	65.64%	0.36%
G Data	26.86%	26.43%	79.94%	22.96%
GFI	3.47%	2.98%	20.90%	6.53%
Hauri	5.70%	4.56%	5.14%	23.63%
Ikarus	5.74%	5.45%	77.17%	22.62%
Kaspersky	6.75%	6.31%	26.02%	5.14%
Microsoft	4.60%	4.56%	11.76%	0.04%
Norman	4.78%	4.36%	25.89%	4.23%
Preventon	7.89%	7.55%	38.77%	13.58%
Quick Heal	26.91%	21.72%	22.85%	7.43%
Roboscan	4.81%	5.31%	3.42%	9.73%
Sophos	6.78%	6.23%	38.58%	5.02%
SPAMfighter	7.18%	6.73%	23.50%	7.87%
Symantec	10.23%	8.52%	21.60%	1.55%
Tencent	8.98%	9.31%	59.68%	193.82%
Total Defense	25.47%	25.65%	46.80%	10.36%
TrustPort	9.95%	11.66%	42.66%	15.92%
UtilTool	7.40%	6.76%	33.96%	4.17%
VirusBuster	5.57%	5.21%	23.83%	7.05%

Please refer to text for full product names.





averaging around six minutes in total. An option to take part in a ‘Signature Quality Assurance Program’ (presumably another of the now ubiquitous feedback schemes) is hard to spot during the install process, being greyed out if the default update settings are accepted.

The interface itself uses the .NET framework and is thus a little wobbly at times, but seems to have improved greatly over the years, in stability if not in appearance. Fairly basic options are provided, but operation is pretty straightforward and requires minimal brainwork.

Scanning speeds were slow over archives and binaries but pretty quick elsewhere, with a similar pattern in the lag times, which were very heavy in the first two parts but not too bad over the remainder of the speed samples. RAM use was OK, CPU use very high, and our set of tasks took a fair while to get through.

Detection rates were very good indeed though, with some excellent scores in the RAP sets and impressive rates throughout the Response sets too, and with no problems in the clean sets (where issues have been all too common in the past) and nothing to complain about in the WildList sets either, *Ikarus* comfortably earns a VB100 award. The vendor now has two passes and two fails from the last six tests; four passes and two fails in the last two years. This month’s performance earns the product a ‘solid’ rating for stability.

Kaspersky Endpoint Security 8 for Windows

Product version: 8.1.0.646

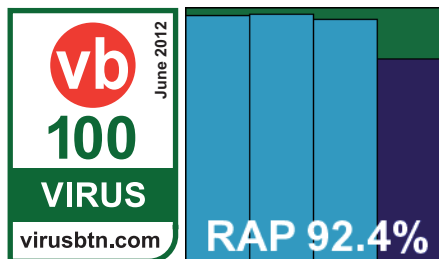
Update versions: N/A

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

False positives 0

One of our most venerable participants, *Kaspersky* maintained an unbroken run of appearances in our comparatives from the

very start until a fateful day a couple of years ago, but has returned to reliable appearances ever since. The company’s business product was provided as a hefty 242MB install package, with a mirror of the full update system at 259MB but including a wide range of additional data. Setting it up required going through a fair number of steps but it only



took a couple of minutes, including the building of a list of ‘trusted’ applications at the end. Updates were mostly fairly speedy but on one install they took over 15 minutes to complete, bringing the average up to seven minutes.

The interface is a little quirky, with some of the on-demand scan options hidden away separately from the rest of the controls, but with a little exploration and practice it soon becomes simple to operate, and it remained solid and stable throughout testing. Scanning speeds were rather slow, especially in the set of miscellaneous file types where we saw a total freeze in the last test, but they were much quicker over media and documents. Overheads were pretty light throughout, the only exception being archive files once the settings had been turned up to extremes. Resource use was fairly average, and our set of tasks ran through nice and quickly.

Detection rates were as splendid as we have come to expect, challenging the very best this month including some multi-engine solutions, and Response scores were solid too. With nothing of note in the clean or WildList sets, a VB100 award is duly granted. Stability was rated a firm ‘solid’, and in our test history for the company’s business line we see three passes and two fails in the last year; eight passes and three fails from 11 entries in the last two years.

Microsoft Forefront Endpoint Protection

Product version: 2.1.1116.0

Update versions: 1.123.1747.0, 1.127.1440.0,

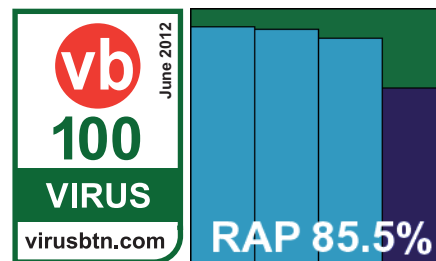
1.127.1739.0, 1.127.1848.0

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.86%

False positives 0

Microsoft has a much less lengthy history in our tests than many, but has established itself as a major heavyweight player in many

regions, at the same time building an appropriately strong history of performances in our tests. The vendor’s business solution, *Forefront*, remains light though, with the main installer under 20MB, and offline updates at 65MB. Set-up is simple and very quick, with updates also speedy, the full process averaging less than two minutes across multiple installs with no reboots required.



Response tests	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
Agnitum	67.13%	72.56%	59.63%	64.66%	62.25%	73.11%	65.71%	66.43%
Avast	70.86%	82.16%	71.86%	67.34%	65.91%	63.83%	80.40%	71.77%
AVG	73.38%	91.34%	83.29%	88.37%	78.68%	87.09%	85.64%	83.97%
Avira	73.39%	91.54%	83.51%	88.99%	80.15%	87.97%	87.01%	84.65%
Bitdefender	71.93%	89.75%	78.68%	83.91%	79.40%	87.30%	85.42%	82.34%
Bkis	88.10%	86.25%	92.25%	85.69%	88.49%	85.05%	90.94%	88.11%
BullGuard	71.98%	89.93%	78.68%	84.04%	79.43%	87.39%	85.43%	82.41%
Central Command	66.67%	72.13%	59.33%	64.44%	61.71%	71.96%	65.50%	65.96%
Clearsight	66.64%	70.82%	59.13%	64.34%	61.50%	70.72%	65.38%	65.50%
Commtouch	73.00%	89.79%	78.54%	71.45%	72.99%	75.60%	76.61%	76.85%
Defenx	67.13%	72.56%	59.63%	64.66%	62.25%	73.11%	65.71%	66.43%
Digital Defender	67.61%	76.42%	75.55%	65.60%	65.06%	72.41%	66.48%	69.88%
eEye	83.76%	86.21%	82.26%	83.86%	84.63%	87.39%	85.50%	84.80%
Emsisoft	87.96%	86.09%	92.15%	85.18%	87.92%	84.62%	90.55%	87.78%
eScan	50.13%	52.93%	52.37%	45.59%	59.92%	57.15%	74.54%	56.09%
Eset	71.63%	91.02%	82.15%	85.93%	76.54%	84.38%	82.75%	82.06%
ESTsoft	55.31%	64.25%	54.15%	61.74%	62.26%	70.41%	65.11%	61.89%
Fortinet	73.34%	91.33%	83.57%	88.60%	78.64%	87.45%	84.86%	83.97%
Frisk	45.88%	54.70%	53.03%	52.38%	59.95%	63.52%	65.85%	56.47%
G Data	86.76%	90.54%	92.77%	85.04%	86.18%	86.37%	80.95%	86.94%
GFI	69.64%	89.85%	89.80%	92.02%	82.69%	85.53%	75.64%	83.60%
Hauri	64.89%	54.36%	61.99%	62.80%	70.96%	65.25%	69.32%	64.22%
Ikarus	87.95%	86.06%	92.13%	85.09%	87.91%	84.62%	90.54%	87.76%
Kaspersky	87.53%	84.17%	91.67%	84.42%	87.40%	82.66%	89.58%	86.78%
Microsoft	67.31%	81.46%	87.31%	89.57%	81.93%	81.67%	81.48%	81.53%
Norman	83.52%	84.01%	89.23%	79.07%	80.00%	79.23%	81.47%	82.36%
Preventon	66.64%	70.82%	59.13%	64.34%	61.50%	70.72%	65.38%	65.50%
Quick Heal	61.41%	77.00%	65.59%	67.48%	56.37%	55.67%	74.17%	65.38%
Roboscan	55.31%	64.31%	54.12%	61.78%	62.26%	70.39%	65.04%	61.89%
Sophos	68.46%	90.63%	88.90%	88.13%	81.14%	86.23%	75.97%	82.78%
SPAMfighter	67.61%	76.42%	75.55%	65.60%	65.06%	72.41%	66.48%	69.88%
Symantec	67.44%	62.15%	71.52%	69.72%	66.45%	68.76%	75.06%	68.73%
Tencent	85.67%	92.07%	85.33%	88.39%	84.79%	90.67%	80.79%	86.82%
Total Defense	53.33%	55.15%	50.14%	52.22%	51.87%	54.15%	53.10%	52.85%
TrustPort	74.04%	91.94%	84.04%	88.92%	80.40%	88.02%	87.50%	84.98%
UtilTool	66.64%	70.82%	59.13%	64.34%	61.50%	70.72%	65.38%	65.50%
VirusBuster	66.74%	72.16%	59.44%	64.48%	61.78%	71.98%	65.50%	66.01%

Please refer to text for full product names.

Operation is similarly straightforward, with a fairly limited set of controls but the basics well covered, and stability was fine throughout. Scanning speeds were mostly decent, a little slow over archives which were delved into deeply by default, while lag times on access were barely noticeable. Resource use was low and our set of tasks blazed through in very impressive time, some runs completing quicker than some of our baseline measures and the average only just tipping over into positive numbers.

Detection rates were pretty good too, snapping close at the heels of the leading pack in the RAP sets and very respectable throughout the Response sets. With the core sets properly handled a VB100 award is comfortably earned by *Microsoft*. The product is also awarded another ‘solid’ stability rating, and in our history for *Forefront* (which usually only appears in server tests) we see two passes from two entries in the last six comparatives; five from five in the last two years.

Norman Endpoint Protection

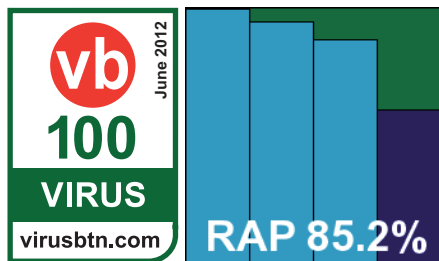
Product version: 9.00

Update versions: 6.08.06

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

False positives 0

Another long-standing regular, *Norman*’s business product seemed little different from its home-user offerings. The



228MB install package provided included latest updates and ran through the standard stages with just a couple of pauses, seeming to complete within a minute or so. This appearance was a little deceptive though, as things continued to be worked on in the background, the product itself not being fully ready for several more minutes after the install interface shut down.

The product’s own GUI is a little challenging, displaying in a browser-type setting and suffering from the difficulties of working in such a format. Settings changes were frequently lost thanks to changing pages without clicking the ‘save’ button (no warning was presented to prevent such errors), and occasionally lengthy loading periods had to be endured. The most glaring issue with it, however, was the

requirement to click through no fewer than seven JavaScript error messages every time the interface was opened. For on-demand scans a proper interface was presented after running a right-click scan, which was then used for all further jobs.

Scanning speeds were pretty sluggish over archives, and also slow in the set of binaries, but they were reasonable elsewhere. Overheads were a little on the high side throughout. RAM use was low though, and CPU use pretty decent too, with our set of activities completed in good time. Detection rates continue to impress, having improved markedly in the last few tests, now threatening to catch up with the leading performers. The WildList and clean sets were dealt with without issues, and *Norman* earns a VB100 award, along with a ‘stable’ rating mainly thanks to interface wobbles. In our test history, *Norman* has five passes and one fail in the last six tests; ten passes and two fails in the last two years.

Preventon Antivirus for Server

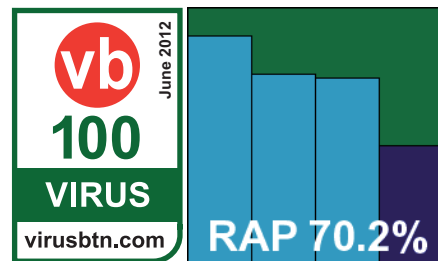
Product version: 4.3.89

Update versions: 14.2.31, 15.0.46, 15.0.51, 15.0.53

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.86%

















False positives 0

Parent of a couple of products already discussed here, with more still to come, *Preventon* has become a regular fixture



on our test bench with its solution based on the *VirusBuster* engine. As usual, the installer measured around 90MB and ran through the standard set of steps to complete in good time, needing no reboot; updates averaged less than two minutes.

The interface is fairly simple and basic, providing no more than the minimum set of options. Some server admins may find this restricting, but the product generally responded well, suffering a few minor issues previously mentioned many times, most notably ignoring its own settings when running right-click scans. Speeds were decent and overheads not bad either, with resource use a tiny bit higher than many, and impact on our set of activities similarly slightly above average.

Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Agnitum		89.77%	75.69%	74.76%	80.07%	50.00%	72.56%
Avast		98.18%	97.99%	94.97%	97.05%	70.77%	90.48%
AVG		99.06%	96.97%	94.05%	96.69%	70.69%	90.19%
Avira		99.20%	97.90%	95.65%	97.58%	81.68%	93.61%
Bitdefender		99.30%	98.71%	97.13%	98.38%	78.18%	93.33%
Bkis		N/T	N/T	N/T	N/T	N/T	N/T
BullGuard		99.36%	98.78%	97.26%	98.47%	78.33%	93.43%
Central Command		89.17%	75.06%	73.14%	79.12%	48.51%	71.47%
Clearsight		88.72%	73.93%	72.19%	78.28%	45.85%	70.17%
CommTouch		87.57%	53.59%	70.26%	70.47%	58.12%	67.38%
Defenx		89.78%	75.69%	74.76%	80.08%	50.00%	72.56%
Digital Defender		88.72%	73.93%	72.19%	78.28%	45.85%	70.17%
eEye		68.87%	97.06%	90.15%	85.36%	62.03%	79.53%
Emsisoft		99.39%	98.54%	96.08%	98.00%	74.85%	92.22%
eScan		99.32%	98.77%	97.04%	98.38%	77.78%	93.23%
Eset		94.68%	88.75%	85.85%	89.76%	78.45%	86.93%
ESTsoft		98.99%	98.39%	96.04%	97.81%	76.85%	92.57%
Fortinet		99.08%	95.41%	95.37%	96.62%	77.08%	91.74%
Frisk		81.48%	41.46%	67.74%	63.56%	52.52%	60.80%

N/T - Not testable.

Please refer to text for full product names.

Detection rates were not very impressive but fairly respectable, with again some problems completing the RAP tests since scans binned out without notice when encountering some nasty samples. No issues were encountered in the core certification sets, earning *Preventon* another VB100 award. With a rating no higher than 'stable' thanks to a couple of minor interface issues, the product's history looks decent with five passes from five entries in the last six tests; seven passes and two fails from nine attempts in the last two years.

Quick Heal AntiVirus – Server Edition

Product version: 13.00(6.0.0.4)


















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

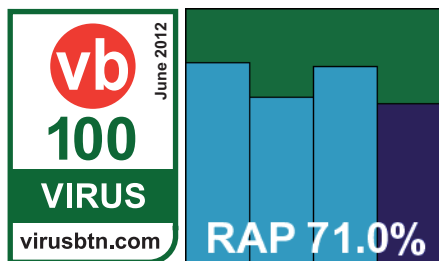
Quick Heal's VB100 history is another that stretches far back into the mists of time, and after a run of considerable

Reactive And Proactive (RAP) tests contd.	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
G Data		99.89%	99.75%	98.45%	99.36%	80.01%	94.53%
GFI		98.91%	92.64%	89.13%	93.56%	63.64%	86.08%
Hauri		99.35%	98.76%	97.36%	98.49%	78.45%	93.48%
Ikarus		99.38%	98.53%	96.05%	97.99%	74.83%	92.20%
Kaspersky		97.00%	97.21%	95.25%	96.49%	79.93%	92.35%
Microsoft		92.81%	91.91%	88.24%	90.99%	68.91%	85.47%
Norman		99.30%	94.47%	87.25%	93.67%	59.59%	85.15%
Preventon		88.72%	73.93%	72.19%	78.28%	45.85%	70.17%
Quick Heal		78.87%	65.43%	77.05%	73.78%	62.77%	71.03%
Roboscan		98.99%	98.39%	96.04%	97.81%	76.85%	92.57%
Sophos		89.11%	72.34%	85.79%	82.42%	69.13%	79.09%
SPAMfighter		88.33%	73.27%	72.01%	77.87%	45.85%	69.87%
Symantec		N/A	N/A	N/A	N/A	N/A	N/A
Tencent		99.26%	97.91%	95.42%	97.53%	80.66%	93.31%
Total Defense		65.53%	63.22%	58.07%	62.27%	45.14%	57.99%
TrustPort		99.89%	99.78%	99.34%	99.67%	84.71%	95.93%
UtilTool		88.72%	73.93%	72.19%	78.28%	45.85%	70.17%
VirusBuster		89.19%	75.07%	73.16%	79.14%	48.52%	71.49%

N/A - Not tested, at request of submitter.

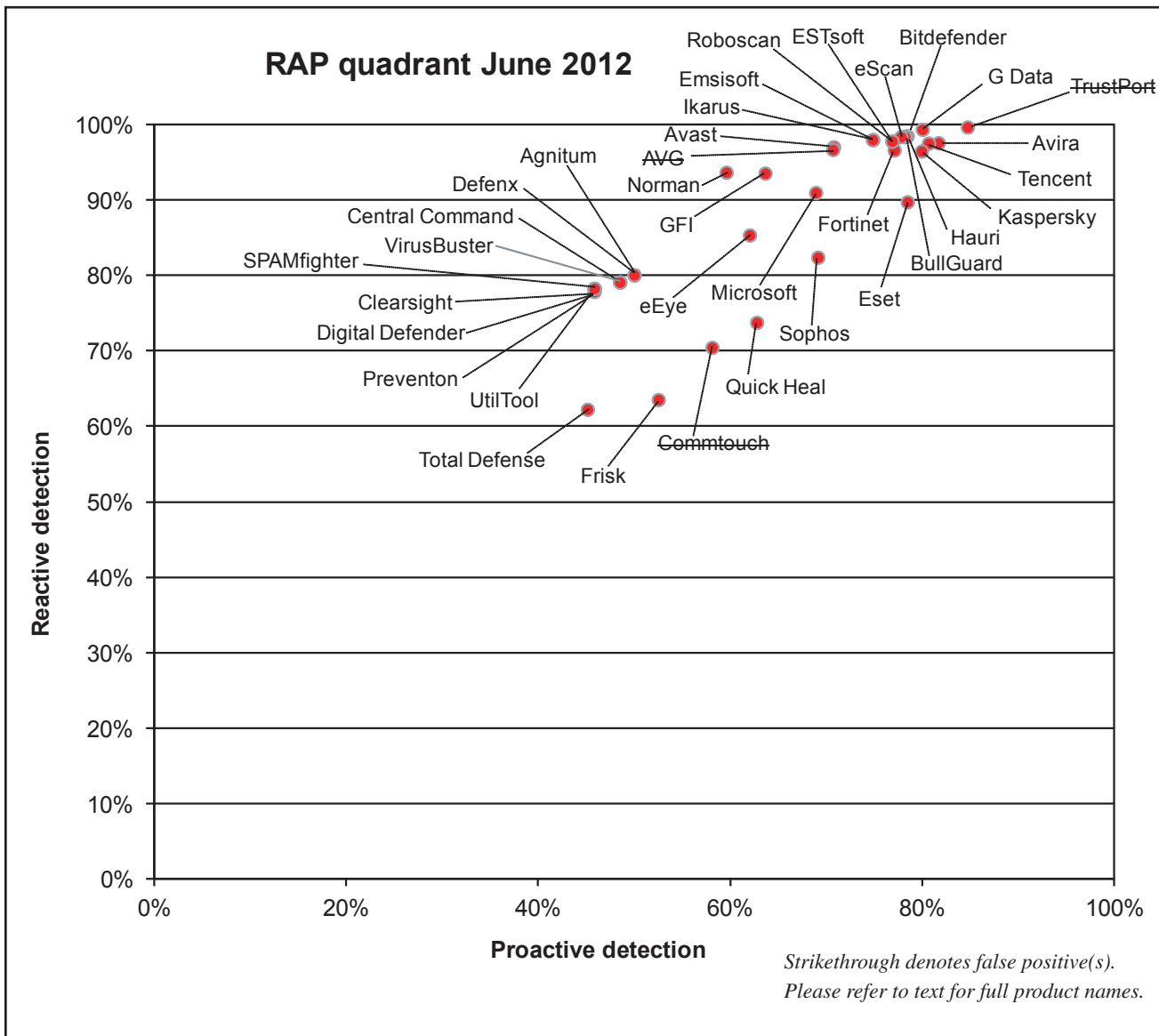
Please refer to text for full product names.

reliability a rocky patch has emerged in the last few tests. The latest version for servers came as a large 307MB installer, which set up in good time with little interaction required,



completing in under a minute with no reboot called for. On one install, updates repeatedly failed, but after waiting half an hour for some unknown issue at the server side to resolve, everything seemed fine; other installs managed to update in minutes.

Scanning speeds were pretty quick, and overheads were pleasingly light too, although RAM use was high: CPU use was not much above average though, and our set of tasks got through fairly quickly. Detection rates were not too great in either the RAP or Response sets, but the core WildList



and clean set presented no shocks, bringing a brief spell of misfortune to an end and earning *Quick Heal* another VB100 award. Stability this month was rated 'solid', and things seem to be back on track with three passes and two fails in the last six tests; nine passes from 11 attempts in the last two years.

Roboscan Enterprise Solution

Product version: 2.5.0.18
 Update versions: 12.3.20.1/425083.2012041810/7.41933
 /7073173.20120417, 12.3.20.1/432196.2012060719/7.42
 498/726393.20120606, 12.3.20.1/432664.2012061116/7.
 42555/7277649.20120611, 12.3.20.1/433117.201206131
 8/7.42574/7280998.20120612

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

Roboscan makes its first full appearance in a comparative this month, although its first submission was actually in the previous

vb June 2012
100
VIRUS
 virusbtn.com

RAP 92.6%

test, when we were unable to coax it into operating properly. Essentially a clone of *ESTsoft's ALYac* targeting western markets, it is based on the *Bitdefender* engine with some additional detection technology courtesy of the Korean sister company. The installer measured 138MB, and presented no surprises with the steps that were run through, completing in a minute or so with an offer to open the product interface – which then failed to appear. Opening it manually proved more effective however, and testing proceeded unimpeded. Updates were once again rather worrying, running through a large number of data files and threatening to come to an abrupt and unannounced stop at any moment, but this time each run seemed to complete without issues, and on comparing the version details recorded in the process of compiling this report, they seem to have been much more successful than *ESTsoft's* own.

The GUI is almost identical to that of *ALYac*, with only branding changes, and is reasonably clear and well laid out with a decent basic level of controls. Testing proved unproblematic, with impressive scanning speeds including improvements in the warm runs, light overheads and very low resource usage, with our set of activities running through quickly. Detection rates in the RAP sets were excellent, but once again the Response scores were way off the mark, implying that the updates had been less successful than they appeared. With the core sets handled properly though, *Roboscan* manages to earn a VB100 award at its first proper attempt. That makes the vendor's first entry in our official test history look good, but it should be noted that a submission in the last test was discounted after we failed to get the product to function sufficiently well to include it in the report. Stability was much better this month, but some suspect updating behaviour marks it down to merely 'stable'.

Sophos Endpoint Security and Control

Product version: 10.0.3/10.0.5

Update versions: 3.30.0/4.76G, 3.31.20/4.78G

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

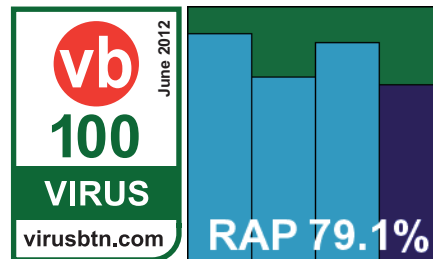
ItW Extd 100.00% **ItW Extd (o/a)** 100.00%

False positives 0

Back to more familiar fare, the latest offering from *Sophos* came as a fairly small 103MB installer, with updates very compact at just 3MB. The installation process was fairly standard and speedy, running through in under a minute with no need to reboot, and updates were also pretty zippy.

The interface is businesslike and efficient, simple to operate and navigate with an enormous wealth of fine-tuning available, and it ran smoothly throughout testing. Scanning

speeds were a little slow over archives (which are scanned fairly deeply by default), and not super quick over binaries and similar items either, but they were fairly quick elsewhere, with lag times on access showing a similar pattern. RAM use was fairly low, CPU use a little above average, and impact on our set of tasks fairly light.



Detection rates were not bad – more impressive in the proactive week than elsewhere in the RAP sets, but Response scores were rather better thanks to cloud look-ups. The WildList and clean sets presented no issues, and a VB100 award is earned with minimal fuss. The product earns a 'solid' rating for stability this month, and in our test history we see four passes and two rare fails in the last year; ten passes in the last dozen tests.

SPAMfighter VIRUSfighter Pro

Product version: 71.176

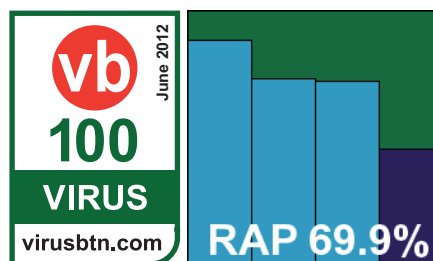
Update versions: N/A

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

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

False positives 0

Another from the *Preventon/ VirusBuster* stable, albeit with a slightly different approach to the interface, *SPAMfighter's* products have



become a fairly regular sight on our test bench in recent years. Slightly larger than its cousins at 94MB, the install package ran through a similar process, the only exception being the request for an email address. The process completed in good time with no reboot required. Operation is fairly simple, with the interface pretty clear and well laid out, providing only basic controls. Stability was mostly OK, although when running scans of large (or even only fairly large) sets of malware the whole interface invariably froze up, requiring a reboot to return the system to full operation.

On some occasions this proved frustrating, as the frozen on-access alert dialog covered the reboot dialog, which on this platform demands a reason for restarting the system, thus preventing a normal manual restart.

Otherwise there were few issues though, with scanning speeds not too bad, overheads a little heavy in places but reasonable in others, and the expected mediocre detection rates. Again, RAP tests took some effort to complete after initial runs crashed out multiple times in one particular cluster of samples. The core sets were properly dealt with though, and a VB100 award is earned. A stability rating would be no more than ‘fair’, thanks to a number of issues. In our test history, five passes from five entries in the last six tests looks good; longer term we see six passes and two fails in the last two years.

Symantec Endpoint Protection

Product version: 12.1.1000.157 RU1
 Update versions: 06 June 2012 r34, 10 June 2012 r17, 11 June 2012 r34

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

False positives 0

Symantec has become something of a rare sight in our tests of late, its corporate solution having last appeared over a year ago. Returning to the test bench, an ample instruction document was provided to assist us in setting up and operating the product, which was very welcome but not really necessary for most tests, as all seemed relatively clear and straightforward. The installer was a fair size at 175MB, but ran through only a few stages including the offer to ‘join the fight against Cybercrime’, with the whole process including updates completed in under two minutes.



The interface is colourful but maintains a professional air, providing an excellent level of configuration in an accessible format. Parts of the interface met with rather surprised nods of approval from some members of the lab team, and it seemed to remain solid under pressure throughout testing. Scanning speeds were reasonable to start with but zoomed through the warm runs, while overheads were mostly light, increasing only when the archive scanning settings were turned up to the max.

The product did not participate in the RAP tests at the request of the submitters, as a considerable amount of its detection is provided by cloud look-ups, but scores in the

Response test were respectable. The WildList sets were handled well, and the clean sets produced only ‘suspicious’ type alerts, most of which were labelled simply ‘Suspicious. Cloud’. These included a large number of components from a single package, *Adobe Reader 9.0*, as well as some other fairly well-known items such as *Skype*, *Microsoft’s SharePoint* and *IBM’s Lotus Notes*, with the remainder made up from various free and shareware items (many of which may well have suspicious components). As such alerts are permitted under our rules, a VB100 award is earned with no problems; it’s worth noting that if suspicious alerts were counted when measuring detections, the Response set scores would have challenged the very best this month. Stability was impeccable, earning the product a ‘solid’ rating, but our test history is sparse for this product, this being the only entry in the last six tests; it has three passes from three entries in the last two years.

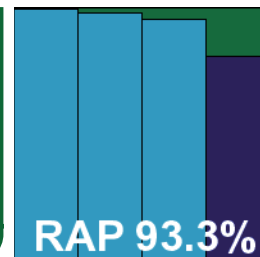
Tencent QQ PC Manager 6.6

Product version: 6.6.2281.201
 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

Tencent is an entirely new name on our roster, although not a complete unknown to the anti-malware world. This is the company behind the



QQ instant messaging system and one of the world’s busiest web portals: the IM program boasted over 700 million active accounts by the end of last year (according to *Wikipedia* at least), while the qq.com website is the eighth busiest in the world at the time of writing, ahead of *Twitter.com* and *Amazon.com*, according to *Alexa* rankings. Outside the company’s native China, *QQ* is also well known to malware researchers as a popular target for worms and data-stealing malware. The company’s anti-malware product is currently available in Chinese only, but from a brief pre-test overview appears to have a wide range of features; we of course mainly focused on the malware detection element, which is based on the *Avira* engine.

The installer provided measured 111MB, putting it among the smaller solutions this month, and the set-up process ran through just a handful of steps, some of which we actually

managed to divine the meaning of. No reboot was needed to complete.

We can say little about the interface, but it looks like a fairly standard design and we were just about able to navigate parts of it using the icons marking different sections. Thankfully, a detailed guide was provided by the developers which helped us through the more complex parts of our task. Scanning speeds were pretty impressive, only archives slowing things down a little thanks to thorough default settings, but the on-access lag times – which appear almost invisible in our charts – should mostly be ignored as the product does no scanning on-read. On-write scanning is clearly a little cumbersome though: our set of activities, which includes a number of copy and write tasks including unpacking of archives, took a very long time to complete. RAM use was fairly low, but CPU use was pretty high.

Detection rates were hugely impressive though, with RAP scores putting the product way up in the top corner of our chart, and Response scores were also excellent. The certification sets were brushed aside effortlessly, and *Tencent*, courtesy of *Avira*, comfortably earns its first VB100 award on its first attempt, along with a ‘solid’ rating for stability.

Total Defense Inc. Total Defense R12

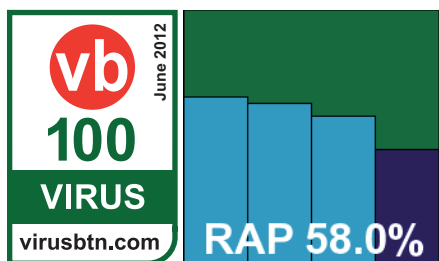
Product version: 12.0.0.833

Update versions: 1.6.0.1884/5778.0.0.0, 5852.0.0.0, 5858.0.0.0, 5863.0.0.0

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

Back to something a little more familiar, *Total Defense Inc.* seems to have completed its separation from *CA*, the originator of this product, and is in the process of splitting up with *HCL*, which was behind much of the development in the past. For now at least, much *CA* branding remains, and the product is essentially unchanged from its first appearance a few years back.

Installation is performed from a full DVD image, although thankfully these days we no longer have to install administration tools first, and for the purposes of the



RAP test updates were taken online on the deadline day. The set-up process is something of a chore, with a lot of information to fill in; some points seem almost deliberately irritating – such as the requirement to select a US state and provide a ZIP code, even after a non-US country has been selected, and the inability of the licensing module to accept the full code in a single paste operation. Once it was all set up though, all updates were reasonably speedy, completing in just a couple of minutes.

The interface is crisp and clear, with a decent level of controls and a fairly sensible layout. It seemed stable throughout testing, and as usual powered through our speed tests in superb time. Overheads were also fairly impressive, slowing down only when archive scanning was enabled on access. RAM use was a little high and CPU use also above average, but our set of tasks got through in decent time.

Detection rates were once again rather poor, coming in well down on the RAP chart, and underwhelming in the Response tests too. However, the core sets were handled better, with no issues in the WildList sets and no false alarms either, thus earning *Total Defense* a VB100 award. Stability, if not necessarily design, was sufficiently impressive to merit a ‘solid’ rating, and in our test history we see four passes and one fail from five entries in the last six comparatives; seven passes and three fails in the last two years.

TrustPort Antivirus 2012

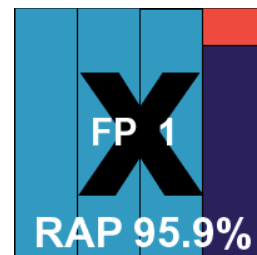
Product version: 12.0.0.4865/12.0.0.4872

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			1

TrustPort is the second of only two products this month to use two separate third-party engines, and once again the high-performing *Bitdefender* engine is in the mix. The latest build came as a 184MB package including updates, and took around a minute to run after the usual handful of stages. Online updates were a little on the slow side, averaging around five minutes thanks to the need to update both components separately. On one occasion an update was requested after an update, but this did not appear to be the norm.

The product has a rather unusual approach to interface design, with no main GUI, but a configuration tool provides



most of the requirements in one spot. Overall, the system is fairly clear and usable, and it responded well under pressure, although as in previous tests we observed some rather odd changes in how windows – of other applications as well as those of the product itself – shifted their focus behaviour after we had run a few heavy tests.

Things moved along well though, with fairly sluggish speeds on demand, and overheads a tad high on access; resource use was above average but not excessive, and our set of tasks didn't take too long either. Detection rates were as amazing as we might expect, with RAP scores some way ahead of a strong field and some very high numbers in the Response sets too. The WildList presented no difficulties, but in the clean sets a single FP, shared with engine provider AVG, was enough to upset *TrustPort's* hopes of a VB100 award this month, as well as earning it a strikethrough on the RAP chart. There were some minor oddities in the system behaviour which were adjudged sufficient to mark it down to 'stable', and our test history now shows two passes and two fails in the last six tests; the longer-term view is better though, with six passes and two fails from eight entries in the last two years.

UtilTool Server Antivirus

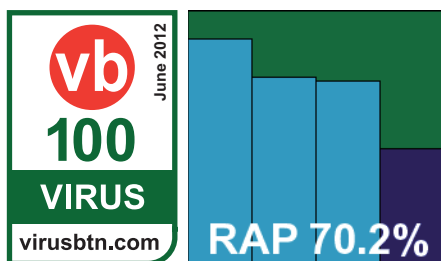
Product version: 3.0.89

Update versions: 14.2.31, 15.0.46, 15.0.51, 15.0.53

ItW Std	100.00%	ItW Std (o/a)	100.00%
ItW Extd	100.00%	ItW Extd (o/a)	99.86%

False positives 0

Another member of the *Preventon!* *VirusBuster* family, *UtilTool* has put in quite a few appearances of late. The



89MB installer produced no surprises, following the standard path in a speedy manner, but the interface was a little different from its sibling products – a slightly newer, somewhat boxier-looking version which we have seen in a few products recently. Operation was much the same however, and updating once again completed in a couple of minutes.

Scanning speeds were reasonable, while overheads were heavy in the archives and binaries but light elsewhere. Resource use was on the low side for RAM, a little high

for CPU and our set of tasks ran through in surprisingly good time. Detection rates were distinctly mediocre almost across the board, the WildList sets being the only exception, and with no issues in the clean sets either *UtilTool* earns a VB100 award. That makes for three passes and a single fail from four entries since the vendor's first appearance under a year ago. *UtilTool* earns a 'solid' stability rating this month.

VirusBuster for Windows Servers

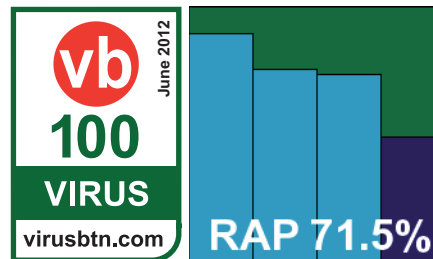
Product version: 7.4.52

Update versions: 5.5.0/14.2.32, 5.5.1/15.0.46, 15.0.51, 15.0.53

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

False positives 0

Finally this month comes *VirusBuster* itself. As ever, it was unlikely to produce many shocks thanks to multiple appearances



of its engine in various guises already. An 88MB install package was combined with 92MB of updates. The set-up process required quite a few steps to be clicked through, but once that was done it completed in good time. Updates were frustrating again – failing initially, but eventually completing happily if left to their own devices. The interface is an MMC monstrosity, the cause of much head-scratching thanks to its unpredictable and inconsistent layout, but it did at least remain fairly stable.

Scanning speeds were impressive in some parts of the test sets, but slow over binaries and archives, with fairly hefty overheads on all but archives, which go unopened even with the setting to inspect them apparently activated. Detection rates were some way off the pace, but just about within respectable limits, and the core sets were managed properly, earning *VirusBuster* a VB100 award. The product maintains an impeccable record of 12 passes out of 12 in the last two years, and earns a 'solid' rating for stability.

CONCLUSIONS

This test has been a much more pleasant experience for us than the last one. It seems rather premature to announce that

our nascent stability rating scheme has reaped miraculous rewards (particularly given that the submission date for this test came before the publication of the last set of results), but we have certainly seen far fewer problems with the product line-up this time. Perhaps that can in part be put down to the platform, with servers requiring much more reliable solutions than can be foisted upon mere members of the public, or perhaps it's no more than good luck that we should have had a relatively smooth run in a month where moving our lab ate up a large chunk of testing time.

Once again, the pass rate is fairly high, compared to an average of around 70% in the last few years. We can only speculate as to the reasons for this, but it seems likely that it is partly due to a shift in focus for the WildList, with the Extended list containing only non-replicating items and few of the tricky polymorphic virus strains which generally wreak havoc making their way onto the standard list. We have also had to be fairly lenient when putting together our Extended sets, as during the ongoing settling-in phase we continue to see changes made and items removed long after the list's official release (further samples were still being struck off even as this final report was being compiled, several months on). We continue to do our best to make sure that our tests are as thorough and stringent as ever, but the VB100 award is, by design, something that any decent solution should routinely pass. So perhaps we shouldn't be surprised to see so many products doing well – perhaps it indicates not so much a marked improvement in products' detection rates, but simply a decrease in errors, blunders and moments of lunacy by the developers (better 'quality' in the 'assurance' sense of the word).

Next up is another *Windows 7* test, with the usual wide range of entries expected on a desktop platform, no doubt including a clutch of new faces. We hope to catch up with our schedule and get this one out in good time, and also to be able finally to finish the details of our stability rating scheme so we can include a nice, easily readable table of results. If there's anything else our readers would like to see documented or tested, we remain, as ever, open to suggestions.

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 Server 2008 R2*, Enterprise Edition, with Service Pack 1. For the full testing methodology see <http://www.virusbtn.com/vb100/about/methodology.xml>.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Perl Developer: Tom Gracey

Consulting Editors:

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *Google, USA*

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 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.