OCTOBER 2012

virus BULLETIN

Fighting malware and spam

ISSN 1749-7027

VB100 COMPARATIVE REVIEW ON WINDOWS SERVER 2003 R2

INTRODUCTION

Tests on server platforms generally provide a little breathing space in the *VB* lab, with not quite so many products to wrestle with as on desktop platforms. With the recent release of *Windows 8* – and along with it a fresh new server edition to investigate – this may well be one of our last visits to the aging but still widely deployed *Windows Server 2003* (which has been superseded by *Server 2008*, released alongside *Windows Vista*; *Server 2008 R2* accompanying *Windows 7*; and now *Windows Server 2012*). The 2003 version remains rather dear to our hearts, running on one of the only permanent *Windows* machines in our otherwise heavily *Linux*-based test lab.

The fallout from recent changes in ownership of several major AV industry players – as mentioned in the last review – was expected to continue to affect this month's test, so the absence of a number of regulars was not too much of a surprise. We did receive unexpected entries from a cluster of OEM solutions though, which brought the numbers up to a final tally of 36 products. With testing already well behind schedule thanks to previous tests overrunning, and test time heavily depleted as a result of duties relating to our annual conference and other important meetings, we decided to exercise a strict policy of dismissing any products that exhibited the extremes of instability noted in the last test.

PLATFORM AND TEST SETS

Preparation of the test systems was a straightforward process, the platform being lightweight and speedy to set up. We applied SP2 – which was released more than five years ago – but no further updates or patches, unless specifically required by the products being tested. A handful of useful tools were also added. System images were taken in a much faster and less bulky process than with the more recent, bloatier server editions of *Windows*, and we moved swiftly on to the preparation of test sets.

The core certification sets centred around the July 2012 WildLists, which were released on 8 August – just over a week before our submission deadline (15 August). Going forward, we are considering adjusting the process for freezing the certification sets to ensure they are sufficiently challenging, but for now at least participants had ample time to ensure coverage, with the certification stages of the test not commencing until early September.

Our clean sets were given the usual trim and tidy up as well as some expansion, with a selection of business-oriented software the main addition this month (to suit the corporate-focused platform). The final tally for the false positive tests amounted to just under 650,000 files, taking up around 180GB of disk space.

Few changes were made to the process for gathering and compiling the RAP and Response sample sets, with the RAP weeks averaging around 15,000 samples after final filtering, and Response sets around 2,000 each. The samples used for our speed and performance measures were largely unchanged, just a slight prune here and there to maintain good balance. With everything in place we wasted no time in cracking on with the tests.

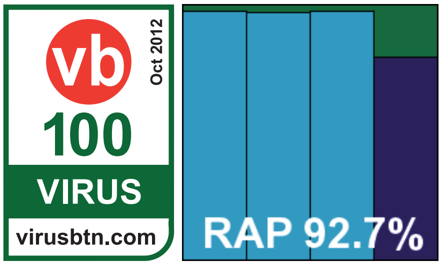
Avast Software Avast! File Server Security

Main version: 7.0.1644

Update versions: 120815-3; 7.0.1646/120910-0

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

Avast! comes first in our list this month, thanks to the absence of a handful of regulars that usually appear ahead of it alphabetically. However, it is often one of the first products we try out in a new test, its reliability, rapidity and ease of use making it ideal for sanity-checking our set-up.



The package provided for this dedicated server edition was a single executable measuring 105MB, and the set-up process is not too different from that of the home-user and free solutions we generally see on our test bench, with plenty of colour and clear, friendly language. It requires only a handful of clicks – rather surprisingly it presents some advertising for a mobile solution, but completes the bulk of the process in less than half a minute. Updates are mostly swift and reliable, although on some occasions an additional ‘program update’ is required alongside the standard data enhancement, and this can take a little longer, with reboots required on some occasions. Nevertheless, few installs took more than two minutes to complete.

The interface is also very similar to other products in the company’s range, with a very clear design and layout, attractive shapes and colours and an all-round pleasant user experience. Configuration is excellent and mostly reliable, although we did have an issue with some of the logging settings, having adjusted the location of the real-time log but finding our changes ignored. Fortunately, logging was gathered properly elsewhere and no data was lost.

Tests blasted through at a zippy pace, with no further issues to report. Scanning speeds were good, lag times fairly low (although this figure is hard to compare with the bulk of the field thanks to there being only minimal on-read protection by default). Our set of activities got through in pretty good time, with reasonable RAM use and CPU use a fraction below the average for the month.

Detection was excellent in the RAP tests, but a little unpredictable in the Response sets, with some days covered notably less well than expected. This dented the averages somewhat, but final scores were still more than respectable. The core sets were handled excellently, and a VB100 award is easily earned. That gives *Avast!* five passes and a single fail in the last six tests; 11 passes in the last two years – a very solid record. Stability was good, with only a minor issue with logging noted, thus earning a ‘stable’ rating.

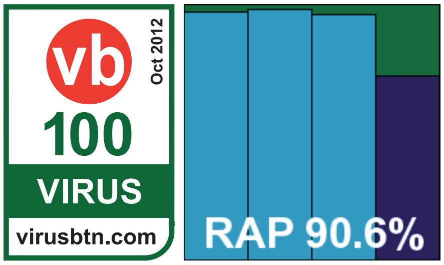
AVG Internet Security Business Edition

Main version: 2012.0.2197

Update versions: 2437/5200, 2012.0.2221/2437/5272, 2441/5277

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

AVG submitted its standard corporate *Internet Security* edition, which was provided as a 171MB executable. Set-up takes a little while, with a few clicks required before the option of an ‘Express’ install path is offered. From there on it takes a little over three minutes for the initial install, and then on completion it runs a quick update, which claims to be complete after only ten seconds or so. If the user then clicks the ‘update’ button, a window opens with a list of updates which are required, and this process takes a little longer (several minutes in some cases, with occasional freezes of the progress screen and other general wobbliness in the interface), and often requests a reboot to complete.



When everything was finally in place, testing proceeded fairly smoothly, with scanning speeds not bad, lag times decent too, and resource use very low indeed; our set of tasks also completed in good time. Detection was decent in the RAP sets, dropping off fairly sharply in the proactive week, and very good in the Response sets, with only a slight decline on the last day. The core sets were again well handled, with no issues in the WildList or clean sets, and *AVG* comfortably earns a VB100 award.

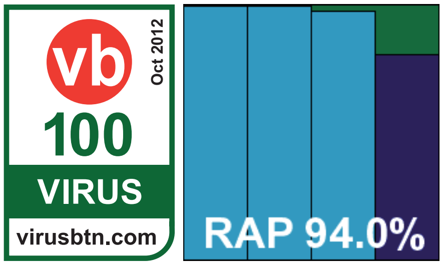
The vendor’s record shows just one fail and five passes in the last six tests; two fails and ten passes in the last two years. With some slight wobbliness during the rather confusing update process, a ‘stable’ rating is earned.

Avira Server Security

Main version: 12.0.0.2309

Update versions: 8.02.10.132/7.11.39.182, 8.02.10.158/7.11.42.206, 8.02.10.162/7.11.43.62, 8.02.10.164/7.11.43.130

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



Another full server solution, *Avira* provided its product as a fairly compact 91MB installer, including all required definition data for the RAP tests. Our first attempt at installing it was aborted fairly speedily, with several messages saying parts of the package could not be unpacked, and there were some rather odd effects on the operation of the desktop. After a reboot however, everything proved perfectly normal, and we were unable to reproduce the oddity over multiple repeat attempts. Under normal circumstances, the install process requires only a couple of clicks and zips through very speedily; updates are so fast it's hard to spot them happening at all, and even with a 'quick scan' at the end the whole process never took more than a minute, with no reboots required.

The interface uses the MMC subsystem, which has caused much displeasure among the lab team in the past, but in this instance it seems fairly well implemented, with navigation and operation fairly simple and user-friendly. Configuration is available in great depth, and responsiveness under pressure seemed good.

Detection was very good indeed, with RAP scores excellent in the reactive weeks and still solid in the proactive part. Response tests maintained a very high level throughout. No problems were noted in the clean sets, and a VB100 award is thus earned without difficulty. *Avira* maintains an impeccable run in our tests with 12 passes in the last two years; this month's performance earns a 'stable' rating, with just the single odd and non-reproducible freak-out at the install stage.

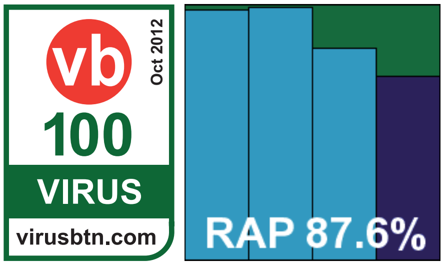
BeyondTrust Blink Server

Main version: 6.00

Update versions: 1.1.2248, 1.1.2303, 1.1.2312, 1.1.2343

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

A few months ago, as part of a swathe of changes across the industry, vulnerability specialist and developer of the *Blink* product, *eEye Digital Security*, was acquired by *BeyondTrust*, a major player in the access control field. We have updated our naming, although there has so far been little change either in the product or in the company websites, other than posts announcing the acquisition. The product has been a regular on our test bench for some time, with this month's submission arriving as a fairly hefty combo of a 264MB main installer and a 162MB update bundle for offline use.



The set-up process is fairly simple and speedy, taking little more than a minute, but initial online updates were rather slow, taking at least ten minutes and sometimes longer. This pushed the overall install time close to a quarter of an hour. On one occasion an update failed to complete successfully, with little information provided, and on repeat attempts it seemed to freeze for some time, finally taking close to 20 minutes to complete.

The product interface is crisp and clear, covering a wide range of security areas of which anti-malware, based on the *Norman* engine, is but a part. Configuration is thus limited by the available space, but a reasonable amount of fine-tuning is provided, and it seems clear and responsive. As noted in past tests, scanning speeds were slow over archives and binaries – where the sandbox solution incorporated in the scanner adds some time to the analysis of unknown items – but reasonable over documents and other items. Lag times were rather heavy but not outrageously so, and while RAM use was fairly low, CPU use was very high. Our set of tasks completed in reasonable time though.

Detection was very good in the earlier RAP weeks, declining steeply into the most recent reactive week and the proactive part of the sets. This impression was confirmed in the Response sets, with fairly unimpressive and rather uneven scores. The core sets were dealt with well though, with no problems in the WildList sets and in the clean sets just a few alerts on suspicious and 'potentially unwanted' items. A VB100 award is thus earned, putting *Blink* on four passes and one fail in the last six tests; eight passes and two fails in the last two years. With just one non-recurring incident noted during an update, a 'stable' rating is earned.

Bitdefender Security for File Servers

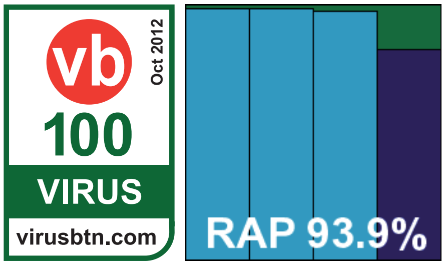
Main version: 3.5

Update versions: 3.5.20.2/7512929, 7547254, 7572488

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

Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Suspicious
Avast	100.00%	100.00%	100.00%	100.00%		
AVG	100.00%	100.00%	100.00%	100.00%		
Avira	100.00%	100.00%	100.00%	100.00%		
BeyondTrust	100.00%	100.00%	100.00%	100.00%		3
Bitdefender	100.00%	100.00%	100.00%	100.00%		
BullGuard	100.00%	100.00%	100.00%	100.00%		
Clearsight	98.25%	95.89%	98.07%	95.84%		
Commtouch	100.00%	100.00%	100.00%	100.00%	5	1
Coranti	100.00%	100.00%	100.00%	100.00%	1	
Digital Defender	98.25%	95.89%	98.07%	95.84%		
Emsisoft	100.00%	100.00%	100.00%	100.00%	1	8
eScan	100.00%	100.00%	100.00%	100.00%		1
ESET	100.00%	100.00%	100.00%	100.00%		4
Fortinet	100.00%	100.00%	100.00%	100.00%		
G Data	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%	1	5
Kaspersky	100.00%	100.00%	100.00%	100.00%		5
Microsoft	100.00%	100.00%	100.00%	100.00%		
Norman	100.00%	100.00%	100.00%	100.00%		
Preventon	98.25%	95.89%	98.07%	95.84%		
Qihoo	100.00%	100.00%	100.00%	100.00%		1
Quick Heal	100.00%	100.00%	100.00%	100.00%		
Sophos	100.00%	100.00%	100.00%	100.00%		
SPAMfighter	98.25%	95.89%	98.07%	95.84%		
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%		
UtilTool	98.25%	95.89%	98.07%	95.84%		
Vexx Guard	98.25%	95.89%	98.07%	95.84%		

(Please refer to text for full product names.)



Bitdefender's submission came as a 191MB executable, which threw us a little right at the start by informing us that our test system was not good enough to host the solution. On closer inspection we quickly realized that it was merely complaining about the absence of the .NET 2.0 framework, and that this was in fact only required to support *Exchange* components. Moving quickly on, the rest of the install process was uneventful, with most defaults set to 'let me decide'. This is another full-blown server solution using the MMC subsystem for its interface, and again despite the lab team's ingrained distaste it was generally found to be pleasantly designed and usable, providing an excellent range of configuration options. At one point we did observe a message complaining about a script error, but for the most part it ran smoothly. Updating was very speedy, taking little more than half a minute even for the initial download.

Scan rates were slow over archives, which are analysed very thoroughly by default, but nice and fast elsewhere, with fairly light overheads, particularly in the warm runs. Resource use was low and our set of tasks got through in good time. Detection was once again superb, with excellent scores in both the RAP and Response tests, both showing just a slight downward trend into the more recent sets.

The certification sets were dealt with efficiently and a VB100 award is well deserved, keeping *Bitdefender* in the elite group of products that can boast 12 consecutive passes in the last two years. With just some minor interface wobbles noted, a 'stable' rating is earned.

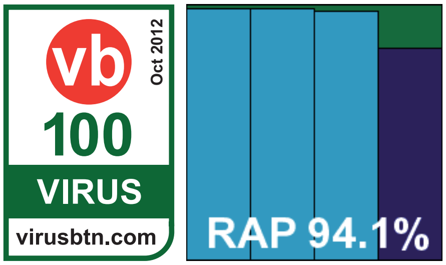
BullGuard Antivirus

Main version: 12.0.230

Update versions: 12.0.0.29/12.0.0.27/12.0.0.58/12.0.0.52

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

A sibling of *Bitdefender* with a similarly strong performance record, *BullGuard*'s product arrived as a 160MB executable including all necessary updates. Set-up requires only a couple of clicks – the standard steps of welcome, choosing options and accepting a EULA all compressed into a single stage – and after ten seconds warned us that a driver for the behavioural component could not be installed (presumably due to a slight incompatibility with the platform, the product's main focus being home users).



The interface is bright and cheery, with a rather unusual approach to design and operation but it provides a good basic set of controls. The real-time section claimed that the on-access component was 'starting' for rather a long time after installation, and accompanying buttons were greyed out, but there seemed to be no interruption in protection.

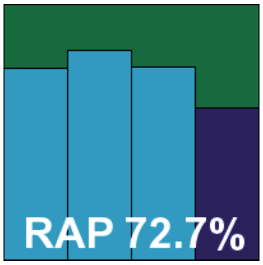
Scanning speeds were very fast, even in initial runs, with warm runs barely measurable, and overheads were pretty light too, again speeding up considerably after a settling-in period. RAM use was around average, but CPU use notably on the high side, while our set of activities got through in decent time. There were no issues in the certification sets, and *BullGuard* comfortably earns another VB100 award. Having skipped a few tests (mainly the annual *Linux* comparative), the vendor remains on nine passes but no fails in the last two years. With little to report other than the unsettling issue with the 'starting' message, a 'stable' rating is earned.

Clearsight Antivirus

Main version: 2.1.91

Update versions: 15.0.147, 15.0.188, 15.0.192, 15.0.194

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Stable



Given the recent upheavals behind the scenes, with engine developer *VirusBuster* handing over control of development and support to *Agnitum*, we were surprised to see entries from the regular cluster of products based on the *Preventon* SDK, but they bravely arrived at the close of the deadline day. First up in this crew is *Clearsight*, which provided a compact 85MB installer for its product. Installation was speedy and simple, and updating seemed fast too, but appeared not to be working properly: after the download stage, a message suggested that the update was complete, but also stated that definition data was well out of date. Repeat attempts didn't help, and only rebooting nudged the display system into updating its message, showing the correct information on the data installed.

With that hurdle out of the way things moved along nicely. The product interface is unchanged and provides a decent basic set of controls in a simple and generally reliable fashion. Speed tests plodded through with scan times a little sluggish and overheads surprisingly high. Resource use was also a little above average, but our set of tasks didn't take too long to complete.

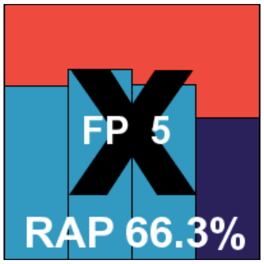
Detection rates were not bad in the earlier part of the Response sets but dropped away fairly sharply; RAP scores were a little unpredictable but also showed a steep dip into the later weeks. There were no problems in the clean sets but the WildList sets showed quite a few misses, improving slightly in later runs but still leaving much to be desired. This might have been expected given the transfer period in the development of the underlying engine. No VB100 award can be given to *Clearsight* this month, but the vendor's record looks quite decent of late, with a single fail and three passes from four entries in the last six tests; seven passes and one fail in the last two years. With some rather odd behaviour during the initial installation, which was repeated on every run, a 'stable' rating is only just earned.

Commtouch Command Anti-Malware

Main version: 5.1.16

Update versions: 5.3.14/201208150952, 201209130125, 201209181239, 201209190937

ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives	5	**Stability**	Solid



It's all change at *Commtouch* too, with the acquisition of *Frisk* meaning that it is now the owner of the engine it formerly made use of as a third-party offering. Ties between the two firms have long been close though, and the merging of teams appears to be going smoothly. The product is generally among the smallest at submission time, this month measuring just 14MB for the main installer and offline updates weighing in at 28MB.

Set-up is simple and speedy with just a handful of clicks required, and updates were very fast too, taking under 30 seconds in most instances. The product interface is basic and starting to look a little in need of a refresh, but it provides decent controls and is fairly easy to use, as well as mostly very reliable. Scanning speeds were pretty slow, and overheads very high with most of our lag tests dragging on for quite some time. RAM use was low but CPU use was off the scale, as was impact on our set of activities which took an age to complete.

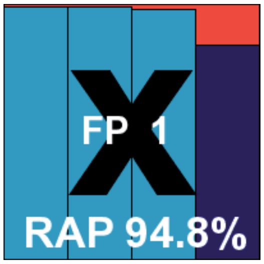
Detection rates were pretty disappointing, as ever, in the RAP sets, but pretty decent in the Response test, illustrating the impact of cloud detection systems. In both cases a slight downward trend was discernible going into the more recent sets. The WildList was well handled, but a small number of items in the clean set were alerted on, all under some vague heuristic or generic flag. These included items from prominent business developers such as *HP* and *Sage*, and were enough to deny *Commtouch* a VB100 award. Luck has been against the vendor of late, with two passes and now three fails in the last six tests; five of each in the last two years. Stability, on the other hand, was excellent, with no issues at all earning the product this month's first 'solid' rating.

Coranti 2012

Main version: 1.005.00006

Update versions: 22852, 23166, 23220, 23251

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



Trouble loomed immediately for *Coranti*, with its multi-engine approach inevitably imposing a higher risk of false alarms and the '*Frisk*' engine one of those included here, alongside *Bitdefender* and *Lavasoft*/*GFI*. The main installer is fairly small, at only 53MB, with a simple and speedy installation process, online updates pulling down just under 240MB of data on each install but not taking too long over it – rarely more than five minutes in total.

The product interface is clear and simple, with a good range of options presented in a fairly easy-to-access, if slightly wordy manner. It operated relatively smoothly, with no issues to report, and demonstrated good scanning speeds with impressive improvements in the warm runs, and fairly light overheads too. Resource use was fairly high, but our set of tasks completed in decent time.

Detection was pretty impressive, with high scores everywhere, dropping off only slightly in the very latest sets. The WildList was handled well, but in the clean sets there

Product information	Install time (mins)	Reboot required	Third-party engine technology	Stability score	Stability rating
Avast	01:10	S	-	1	Stable
AVG	04:30	Y	-	1	Stable
Avira	01:00	X	-	1	Stable
BeyondTrust	14:00	X	Norman	2	Stable
Bitdefender	01:30	X	-	2	Stable
BullGuard	02:00	X	Bitdefender	2	Stable
Clearsight	02:30	X	Agnitum[*]	4	Stable
Commtouch	01:20	S	-	0	Solid
Coranti	06:00	Y	Bitdefender, Commtouch[†], Lavasoft[‡]	0	Solid
Digital Defender	03:00	X	Agnitum[*]	4	Stable
Emsisoft	07:00	X	Ikarus	40	Flaky
eScan	05:50	X	Bitdefender	16	Buggy
ESET	01:00	X	-	0	Solid
Fortinet	01:00	S	-	0	Solid
G Data	15:00	Y	Avast, Bitdefender	6	Fair
Hauri	???	X	Bitdefender	20	Buggy
Ikarus	12:00	X	-	2	Stable
Kaspersky	09:00	S	-	1	Stable
Microsoft	01:30	X	-	3	Stable
Norman	07:00	Y	-	6	Fair
Preventon	02:45	X	Agnitum[*]	4	Stable
Qihoo	03:00	X	Bitdefender	2	Stable
Quick Heal	04:00	X	-	0	Solid
Sophos	03:30	X	-	0	Solid
SPAMfighter	02:20	X	Agnitum[*]	10	Fair
Tencent	03:00	X	Avira	1	Stable
Total Defense	09:45	YY	-	4	Stable
TrustPort	06:30	Y	AVG, Bitdefender	2	Stable
UtilTool	02:25	X	Agnitum[*]	6	Fair
Vexx Guard	02:45	X	Agnitum[*]	6	Fair

S - Reboot required after some updates
O - Reboot optional, only required for some components
YY - More than one reboot required on some installs
??? - Product did not complete install satisfactorily
[*] *VirusBuster engine now owned by Agnitum*
[†] *Frisk engine now owned by Commtouch*

(Please refer to text for full product names.)

[‡] *Lavasoft includes GFI VIPRE*
0 = Solid
0.1 - 4.9 = Stable
5 - 14.9 = Fair
15 - 29.9 = Buggy
30+ = Flaky

On-demand throughput (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Avast	34.71	6.67	6.79	6.67	22.39	23.27	22.39	39.72	87.30	87.71	95.33	95.33	95.33
AVG	40.05	1.58	202.33	1.58	17.99	50.12	17.99	11.21	67.90	24.76	25.94	78.89	25.94
Avira	33.05	4.91	5.02	4.91	44.79	48.33	44.79	22.88	56.72	50.52	90.79	104.95	90.79
BeyondTrust	13.66	3.69	3.67	NA	6.62	6.70	6.62	19.59	46.32	43.25	41.90	45.58	41.90
Bitdefender	15.09	4.62	4.98	4.62	41.27	42.10	41.27	28.04	63.57	61.91	56.91	58.36	56.91
BullGuard	12.29	5.45	1820.96	5.45	41.01	861.16	41.01	52.96	823.75	116.94	105.92	544.73	105.92
Clearsight	24.94	3.52	3.55	NA	18.15	18.46	18.15	21.83	49.34	48.21	32.87	32.13	32.87
Commtouch	23.94	6.90	6.91	6.90	19.55	19.45	19.55	21.18	47.48	46.78	30.50	30.75	30.50
Coranti	17.95	4.53	910.48	4.53	100.24	263.12	100.24	21.34	411.85	47.13	37.75	178.74	37.75
Digital Defender	30.85	3.37	3.46	NA	16.84	17.19	16.84	27.50	61.91	60.72	32.59	32.41	32.59
Emsisoft	34.14	12.14	10.86	NA	33.41	40.39	NA	24.44	57.23	NA	42.37	54.22	NA
eScan	15.54	5.17	7.65	5.17	9.93	10.78	9.93	2.68	6.17	5.91	10.48	10.49	10.48
ESET	34.42	9.15	124.16	9.15	15.07	526.24	15.07	119.16	6314.88	263.12	47.66	326.86	47.66
Fortinet	42.50	11.53	11.72	11.53	14.82	14.69	14.82	49.31	114.82	108.88	47.66	48.68	47.66
G Data	18.59	3.52	1820.96	3.52	17.02	1894.65	17.02	40.28	3790.44	88.94	61.50	1906.56	61.50
Hauri	14.87	6.13	5.15	6.13	20.70	20.82	20.70	10.63	24.19	23.48	14.89	15.31	14.89
Ikarus	15.26	5.20	5.28	NA	16.75	16.87	16.75	33.64	75.78	74.29	52.23	53.71	52.23
Kaspersky	23.40	3.59	1820.96	3.59	18.04	1578.72	18.04	46.13	1722.55	101.85	53.71	602.10	53.71
Microsoft	8.60	3.82	3.68	NA	15.29	17.51	15.29	32.50	75.78	71.76	35.64	37.51	35.64
Norman	8.69	1.31	1.31	1.31	12.97	12.99	12.97	30.10	66.01	66.47	56.91	59.27	56.91
Preventon	24.79	3.38	3.34	NA	16.57	17.19	16.57	26.48	60.53	58.47	37.75	37.75	37.75
Qihoo	18.76	2.96	2.96	2.96	21.12	21.73	21.12	23.44	57.41	51.76	37.75	37.38	37.75
Quick Heal	44.31	5.86	5.64	5.80	28.57	38.58	28.57	66.51	185.73	146.86	108.95	128.53	90.79
Sophos	14.41	2.42	2.43	2.42	23.56	23.92	23.56	52.96	127.15	116.94	69.33	71.05	69.33
SPAMfighter	28.72	3.46	3.46	3.24	17.07	16.69	16.36	44.68	101.31	43.25	30.50	34.25	30.50
Tencent	25.87	2.95	3.12	2.95	8.80	5.48	8.80	12.77	27.38	28.19	45.94	42.68	45.94
Total Defense	39.66	227.62	780.52	4.23	78.94	728.70	64.44	35.75	1114.52	67.18	82.89	602.10	73.33
TrustPort	11.93	5.13	5.13	NA	15.91	16.15	15.91	18.33	46.21	40.48	31.00	31.69	31.00
UtilTool	28.14	3.68	3.75	NA	14.45	14.75	14.45	20.57	47.24	45.43	27.04	27.04	27.04
Vexx Guard	27.22	3.28	3.48	NA	16.79	16.99	16.79	20.00	46.09	44.16	31.26	31.00	31.26

** System drive size measured before product installation.*

(Please refer to text for full product names.)

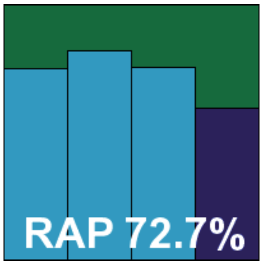
were issues as feared – not as bad as we expected, with just a single full alert, but still enough to spoil *Coranti*'s chances of a VB100 award this month. With a rather sporadic pattern of entries *Coranti* now has two passes and one fail from three appearances in the last six tests; four passes and two fails in the last two years. Stability was not a problem though, with a 'solid' rating earned.

Digital Defender Server Edition

Main version: 2.1.91

Update versions: 15.0.147, 15.0.188, 15.0.192, 15.0.194

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Stable



Another from the *Preventon* stable, *Digital Defender*'s server solution has been seen several times before in these pages. The slim 85MB installer ran well, but as predicted following our earlier encounter with a product from the *Preventon* clan, there were some oddities with the update process, data not righting itself and showing some distinctly worrying information at least until the next reboot. Otherwise operation was decent – scanning speeds were not great but not too bad either, overheads were a little heavy, RAM use was OK but CPU use a bit high, and impact on our set of tasks was not bad.

Detection was reasonable to start with but showed a steady downward slope. There were no false positives, but the WildList sets were handled far less reliably than we require and no VB100 award can be granted to *Digital Defender* this month. That puts it on three passes and a single fail in the last six tests; seven passes and two fails in the last two years. With some issues encountered during the update process, the product just about scrapes a 'stable' rating.

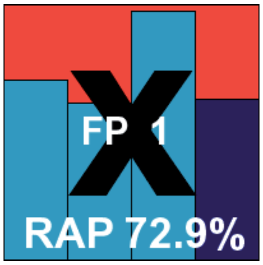
Emsisoft Anti-Malware

Main version: 6.6.0.4

Update versions: 6631272, 7734128, 7827397, 7854621, 10863274

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

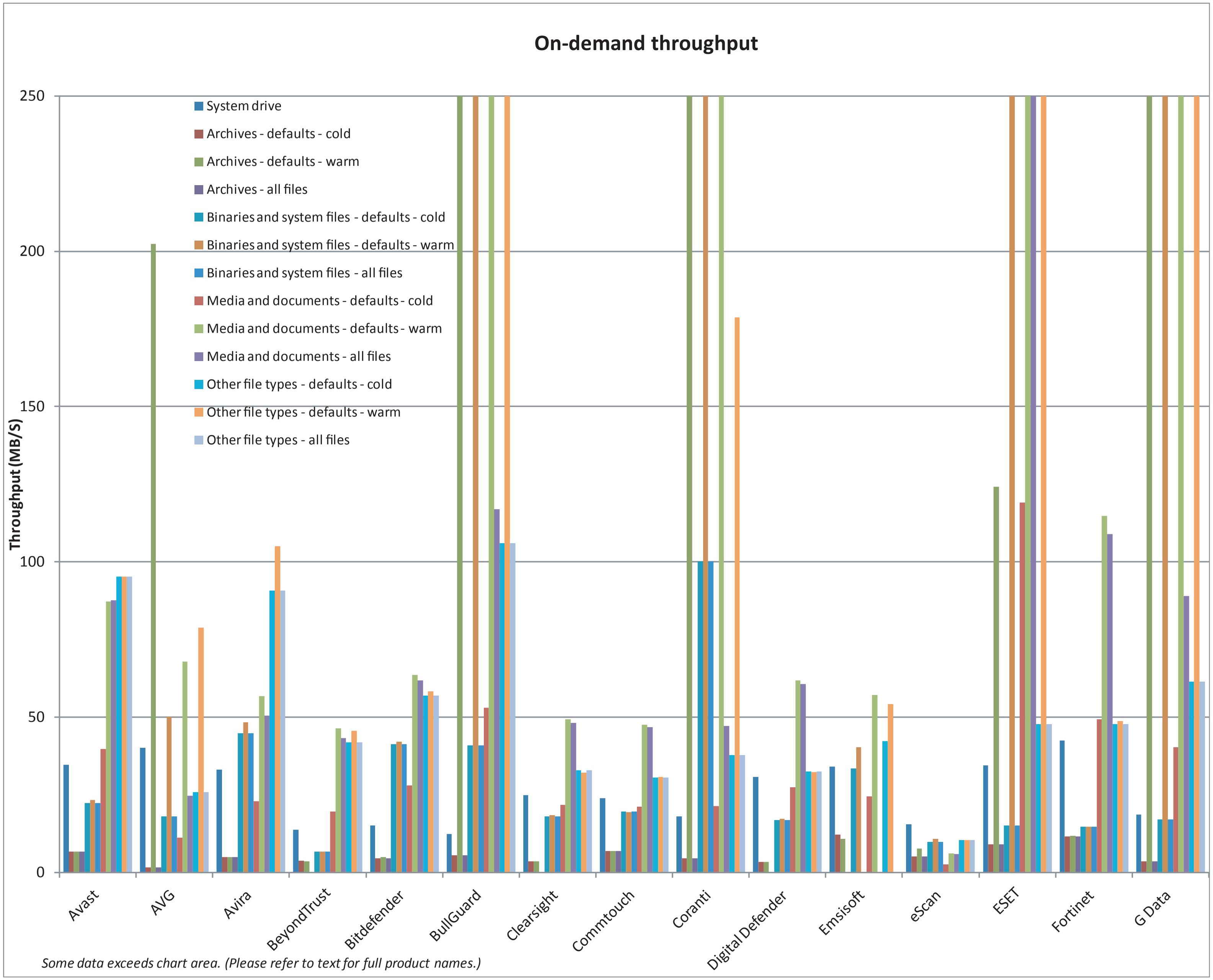
With little changed for now but some major enhancements on the way, *Emsisoft*'s solution will soon boast the *Bitdefender* engine in place of that of its current partner, *Ikarus*. The product installer is a fair size at 151MB, including all the latest data, but initial installation is fairly speedy. Updates are on the slow side though, taking up to five minutes in some cases, and in one instance the update process failed, claiming a lack of Internet connection (although a connection was in place). Re-running the task once the install was complete took some 10 minutes and ended with an error message warning of a 'major problem'. This led to the product interface refusing to open even after a reboot. In the end the decision was taken to retry the install from scratch on a fresh machine, and this time all went perfectly smoothly.



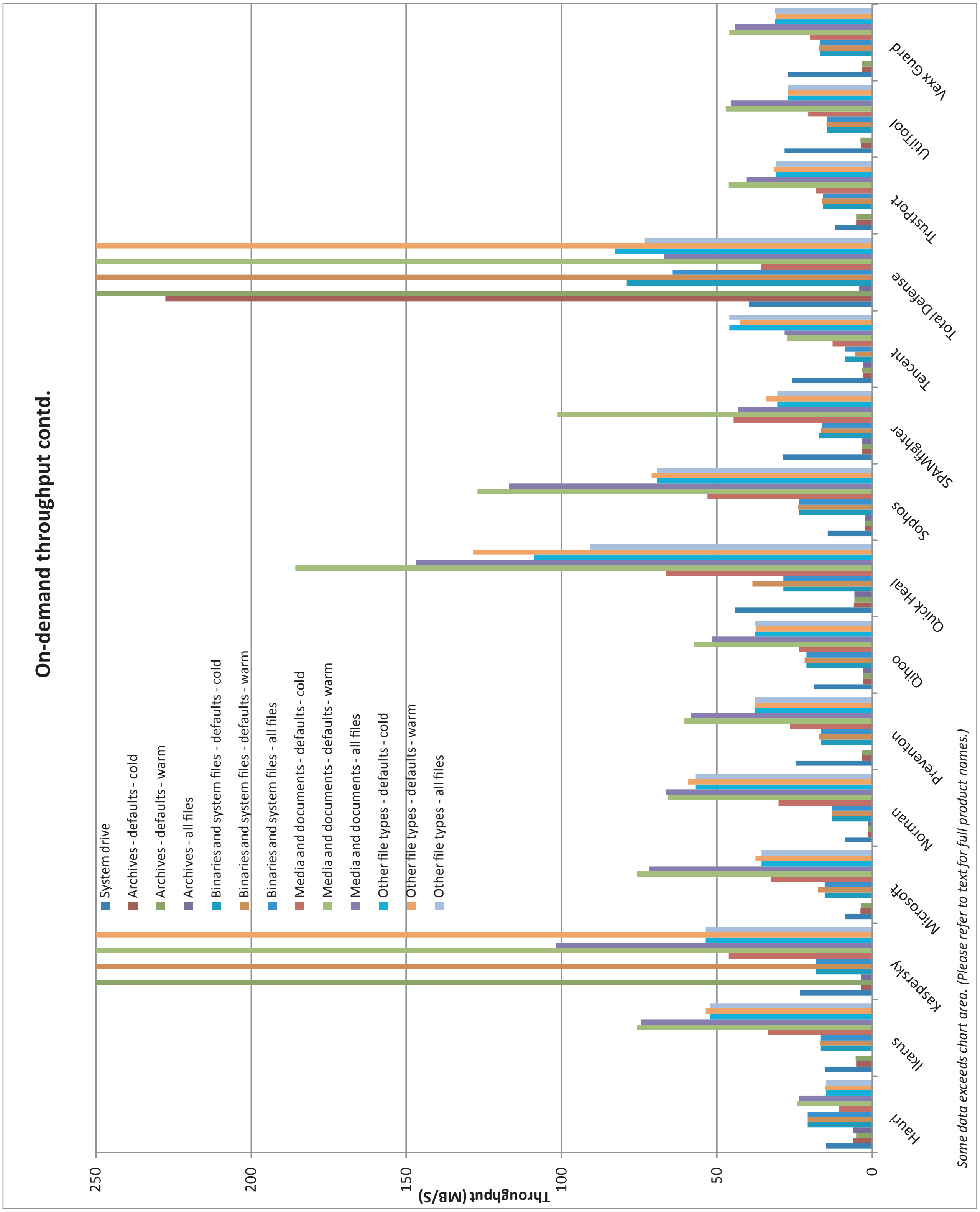
The interface is a little slicker than in past tests but much the same in layout, providing a decent range of controls which are mostly fairly accessible. Scanning speeds were not bad and overheads were reasonable too, with very light RAM use. CPU use was also very low, and our set of tasks took just a little longer than the average for this month.

In the detection tests things were much less smooth however, with many jobs ending with a catastrophic 'a major problem has occurred' message. In some cases this left the product inoperable and protection disabled; in others it was possible to continue working. When things were snarled up a reboot generally cured things, but on at least two occasions even after multiple reboots and attempts to restart various services we were unable to access the product interface, run any scan tasks or find any evidence of active protection – the test system had to be wiped and testing restarted on clean hardware. This made for quite some work. In most cases the problem seemed to be unrelated to the files being scanned, as the same scan could successfully be run to completion on later attempts. However, in some instances, particularly in the RAP sets, it was clear that particular samples were causing issues, with jobs repeatedly stopping in the same places. The developers suggested the issue might be down to the product's quarantine filling up too quickly, but as we routinely disable quarantining and cleaning before running large scans this seemed unlikely to be a factor here.

Efforts were made to cover as much of the test sets as possible, but inevitably some items went unscanned where stability was too shaky to cover much of a folder. This will have impacted detection rates, which were excellent in some sets but a little less solid elsewhere, mainly as a result of the problems encountered. The WildList was not hit by the issues and was covered well, but in the clean sets a single file, part of a business package from *HP*, was alerted on as



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


On-demand throughput contd.

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

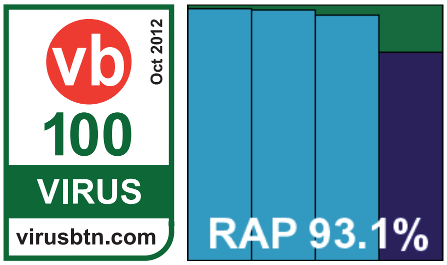
a dropper trojan, and *Emsisoft* does not make the grade for a VB100 award this month. Its ongoing streak of bad luck with false positives puts *Emsisoft* on one pass and four fails in the last six tests; two passes and eight fails in the last two years. With a large number of problems encountered – most of them described by the product itself as 'major' – stability is rated at the lowest level, 'flaky'.

eScan Internet Security Suite

Main version: 11.0.1139.1250

Update versions: NA

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



Another client of the ever-popular *Bitdefender*, *eScan* has been using the engine rather longer and has done pretty well out of the deal. The current version came as a hefty 192MB installer, which took some time and quite a few clicks to get through. The install process is lively, with lots of progress bars, message windows and so on to keep the operator amused. After a couple of minutes of activity it launches straight into a scan, and then is all done. Updates appear not to start automatically (or at least not soon enough for impatient types), so were kicked off manually, taking a further three to four minutes to complete the set-up process.

The interface is glossy and colourful, with some funky buttons which swell up when hovered over like *Mac* menus. The developers have obviously spent a lot of time on this, but their time would perhaps have been better spent looking more closely at the product's operation and messaging: initial tests showed no sign of active protection, and this was only remedied by a reboot, which was not requested at any time by the product itself, yet appears to be essential. On restart, on several occasions we encountered a message warning that the monitoring tray component had experienced a problem – but this didn't seem to affect the protection, which was now fully operational.

Testing advanced more rapidly from here on, with speed and performance measures hitting few snags. Scanning speeds were sluggish and overheads a little high, but resource use was low and there was a low impact on our set of tasks. Detection tests were more difficult, with the interface locking up several times towards the end of larger jobs, and on one occasion, when the product was installed with no Internet connection for the RAP tests, it appeared to detect nothing at all – scans were run over several sets including the EICAR test file, and claimed to have completed successfully with nothing to report. Rebooting and tweaking the settings, and even running online updates appeared to produce no improvement, and in the end we were forced to start again from scratch with a fresh install – fortunately this time everything went smoothly and the previous oddities could not be reproduced.

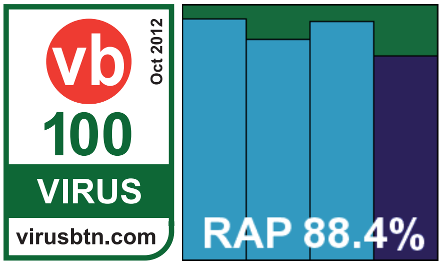
Given the underlying engine it was little surprise that detection rates were excellent, with just a slight drop into the later sets, and the core sets were handled well, comfortably making the grade for VB100 certification. That puts *eScan* on six passes in the last six tests; 11 passes and a single fail in the last two years. However, multiple issues with the product earn it a less than pleasing stability rating of 'buggy' this month.

ESET Endpoint Antivirus

Main version: 5.0.2126.0

Update versions: 7389, 7477, 7389, 7497

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



Another long-term high performer, *ESET*'s latest corporate solution picks up the 'Endpoint' tag which seems to be all the rage these days. It seems fairly similar to the consumer products we are more used to seeing in our tests though, with the svelte 64MB installer starting off by warning that we were installing an endpoint solution on a server, which might be better protected by a dedicated server product. The rest of the set-up was smooth and quick, with updates completed in a flash and the whole process taking under a minute on each install.

The interface is crisp, clean and pleasant, with a splendidly comprehensive set of configuration options, and ran smoothly with no issues throughout testing. Speeds were excellent on demand, particularly in the warm runs, and overheads extremely light; resource use was well below average and our set of activities ran through very quickly indeed.

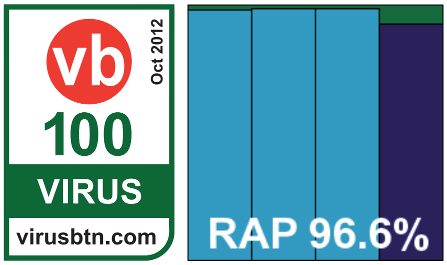
Detection rates were solid throughout, with no issues in the core sets easily earning *ESET* yet another VB100 award – the vendor has entered and passed every *VB* comparative since June 2003. With a very impressive performance this month, a 'solid' stability rating is well deserved.

Fortinet FortiClient

Main version: 4.1.3.149

Update versions: 5.0.26/16.37, 16.386, 16.403, 16.421

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



Fortinet's scores have been climbing steadily of late, from a fairly low spot a year ago to some very impressive heights. The current version was provided as usual as a tiny 10MB installer, with an offline update bundle of 137MB. The set-up process offers the choice of free or premium products, with the latter option selected for testing this month. The process completes after the usual steps in under half a minute. Updates are fast and after some runs request a reboot, the entire install process never taking more than a minute. The design is simple and clear, and the interface proved reliable and responsive throughout testing.

Scanning speeds were pretty good, with overheads a little high to start with but dropping sharply after initial settling in. RAM use was low, CPU use perhaps a little higher than average, but our set of tasks ran through in very good time.

Detection scores were once again excellent across the board, taking a commanding position on the RAP chart, and with no issues in the certification sets a VB100 award is easily earned. Having missed only our annual *Linux* tests, *Fortinet* now has five passes from five entries in the last six tests; nine passes and a single fail in the last two years. This month's splendid performance is capped off with a 'solid' stability rating as we encountered no issues whatsoever.

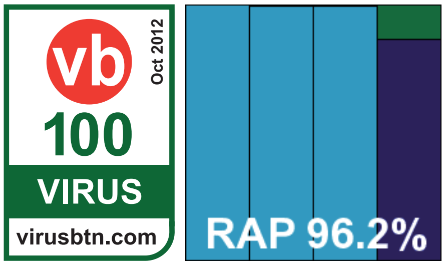
G Data AntiVirus Administrator/Client

Main version: 11.5.2.133

Update versions: AVA 22.5792/AVL 22.1117, AVL 22.1181, AVL 22.1190, AVA 22.6167/AVL 22.1197

G Data AntiVirus Administrator/Client contd.

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



As in several previous server tests, the *G Data* product was provided as a combination of administration system and protection client agent. This made the submission rather large, with the admin kit weighing in at a hefty 659MB, and the client was provided as a separate 215MB package. Installation of the management side of things was fairly simple but did take some time, much of which was devoted to the .NET framework. Once the control system was in place deployment to clients was generally smooth and simple, although the discovery of connected systems seemed more complete on some runs than others. The whole process took between six and eight minutes, with a reboot partway through. Updating was a little harder to measure, as it ran as a background task with little indication of exactly when everything was safely installed, but it seemed to add another seven or eight minutes at least to the total set-up time.

The interface is reasonably easy to navigate but has a tendency to dawdle when refreshing screens and seemed a little shaky at times, as well being rather short on feedback and information. On one install, an on-access run showed some odd results, with protection clearly shutting off for a spell in the middle of the run, possibly while an update was applied. In the on-demand work, a couple of scans stopped short with large chunks of the area we had asked to be checked ignored; in both these cases, re-running the same job worked fine, so the issue was clearly simply one of wobbliness rather than a recurrent bug. Nevertheless, unreliability is not to be expected in a server-grade solution.

Scanning speeds were more impressive, especially in the warm runs, and on-access lag times were also good after more thorough initial checks, which did take some time. Resource use measures appear a little high, but this figure is difficult to compare with other products as the administration suite was installed on the same system as the client and doubtless hogged the bulk of the memory and CPU time taken up. Our set of tasks ran fairly slowly too.

Detection rates were excellent as ever, with RAP scores hard to fault even in the proactive week and Response scores

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
Avast[†]	0.18	1.23	0.63	130.68	22.56	15.32	32.95	1.64	0.33	18.66	1.99	0.58	7.15
AVG	4.57	4.34	2.05	5.21	54.44	12.08	11.81	34.83	21.94	33.28	17.41	12.87	37.25
Avira	9.30	6.17	3.11	58.65	19.91	0.30	22.99	38.40	25.21	36.85	7.86	7.89	7.79
BeyondTrust	35.89	15.63	15.82	NA	93.25	89.85	93.25	48.56	46.37	48.56	21.78	21.14	21.78
Bitdefender	20.17	73.45	0.78	169.99	24.92	0.58	24.84	23.31	16.97	34.89	13.07	9.51	19.31
BullGuard	18.68	184.95	6.76	NA	30.47	2.76	30.47	19.93	2.53	19.93	11.94	1.97	11.94
Clearsight	18.32	83.18	83.38	113.89	52.98	52.76	53.56	20.46	17.20	49.12	12.45	9.05	34.39
Commtouch	13.80	154.57	155.09	153.26	50.72	50.24	50.46	71.85	71.53	70.21	26.26	25.42	25.00
Coranti	7.79	10.96	9.41	18.17	77.67	21.36	28.97	30.43	20.25	56.70	2.81	0.88	19.84
Digital Defender	15.42	85.64	86.27	221.93	79.46	73.06	74.15	3.57	2.16	29.58	2.33	0.76	25.08
Emsisoft[†]	15.90	1.81	1.96	20.83	34.54	11.62	47.13	22.82	21.87	74.27	17.90	13.51	40.36
eScan	42.64	14.98	6.74	25.80	48.80	15.91	55.69	87.62	14.94	88.76	17.80	0.82	58.88
ESET	2.18	1.77	1.42	NA	8.76	1.29	8.76	4.35	3.25	4.35	3.71	1.43	3.71
Fortinet	15.29	85.08	0.80	85.08	69.11	15.99	69.11	11.59	0.13	11.59	16.38	1.36	16.38
G Data	69.42	73.97	3.54	73.97	78.08	19.51	78.08	33.58	2.15	33.58	22.62	3.06	22.62
Hauri	17.01	3.91	2.89	2.69	25.98	15.32	15.34	29.06	24.88	23.96	17.30	14.77	13.52
Ikarus	34.53	183.56	184.39	183.56	57.73	53.26	57.73	21.00	20.05	21.00	17.64	14.26	17.64
Kaspersky	19.30	0.11	0.21	0.88	15.91	16.11	19.50	1.67	1.77	1.57	1.74	1.90	2.42
Microsoft	1.00	4.00	0.69	NA	52.51	0.04	52.51	12.89	1.09	12.89	14.69	0.26	14.69
Norman	18.84	15.56	0.49	NA	90.10	0.27	90.10	33.46	1.70	33.46	24.12	0.94	24.12
Preventon	17.44	81.19	75.59	227.47	55.31	54.47	56.27	4.46	3.32	36.79	2.05	0.78	26.35
Qihoo[†]	6.22	1.80	2.05	NA	12.28	12.04	12.28	22.96	21.93	22.96	13.86	13.09	13.86
Quick Heal	4.35	3.30	3.88	NA	27.65	24.70	27.65	9.40	8.76	9.40	6.73	6.71	6.73
Sophos	19.47	3.61	3.89	388.42	38.82	38.14	41.86	8.21	6.45	13.42	9.13	8.18	13.32
SPAMfighter	15.41	80.22	81.05	106.96	55.27	54.92	56.56	23.08	19.61	49.82	2.12	1.00	30.44
Tencent[†]	9.30	6.98	7.52	NA	17.63	16.38	17.63	22.66	14.95	22.66	1.60	0.79	1.60
Total Defense	16.38	3.98	2.68	225.28	13.85	9.07	14.68	28.52	25.17	33.49	12.48	11.69	13.25
TrustPort	13.37	11.91	2.09	359.36	64.88	12.10	71.38	49.23	23.10	56.25	30.94	14.22	34.65
UtilTool	14.81	89.42	84.04	209.58	67.37	66.31	66.52	25.36	23.57	53.41	14.46	13.53	36.64
Vexx Guard	15.27	87.12	87.50	209.98	55.77	55.47	54.92	23.67	19.67	51.35	2.24	0.99	31.94

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

[†] *No full on-read scanning by default.*

(Please refer to text for full product names.)

splendid across the board. The core sets were well handled and *G Data* earns a VB100 award, putting it on five passes from five attempts in the last six tests; nine passes and one fail in the last two years. Stability was a little questionable this month, with a selection of mostly minor issues mounting up to a score just nudging into 'fair' territory.

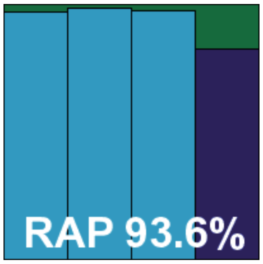
Hauri ViRobot Server Protection 2011

Main version: 6.0.0.0

Update versions: 2012-08-15.00(7512929)

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

vb Oct 2012 100 VIRUS virusbtn.com



Yet another product based on the *Bitdefender* engine, *Hauri* has underperformed in the past thanks to some issues with updating. Hoping for better things this time around, the 182MB install package ran through the usual stages, taking minimal time despite the pre-install scan. On completion it presented the option to run an update. However, this and repeated subsequent attempts to launch updates proved fairly profitless – while a few did at least open a progress dialog with some sign of action, on most occasions very little seemed to happen at all. On all attempts the version information displayed in the main interface failed to change, although on some occasions it was at least marked with a red 'x' to indicate that it was in need of updating; exactly how this is supposed to be achieved remains something of a mystery.

The interface itself is fairly straightforward, providing a decent if not exhaustive set of controls, and it generally seemed to respond well, at least when not being asked to perform updates. At one point a scan of clean items in one of our false positive tests did completely freeze up, but we were able to kill the job and restart it fairly easily once we realized there was a problem. Eventually completing our work, we saw some rather sluggish scanning speeds, reasonable overheads, RAM use slightly above average but CPU use well below, and a fairly heavy hit on our set of activities.

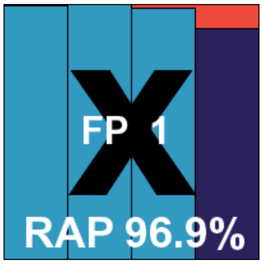
Detection was excellent in the RAP sets but fairly mediocre in the Response sets, confirming our suspicion that updating was once again completely ineffective. The core sets were not affected by this however, and a VB100 award is just about earned, putting *Hauri* on three passes from three attempts in the last six tests; three passes and three fails in the last two years. With a number of issues this month, some of them fairly serious, stability could be rated no better than 'buggy'.

Ikarus anti.virus

Main version: 2.2.12

Update versions: 1.1.122/82051, 82267, 82295, 82312

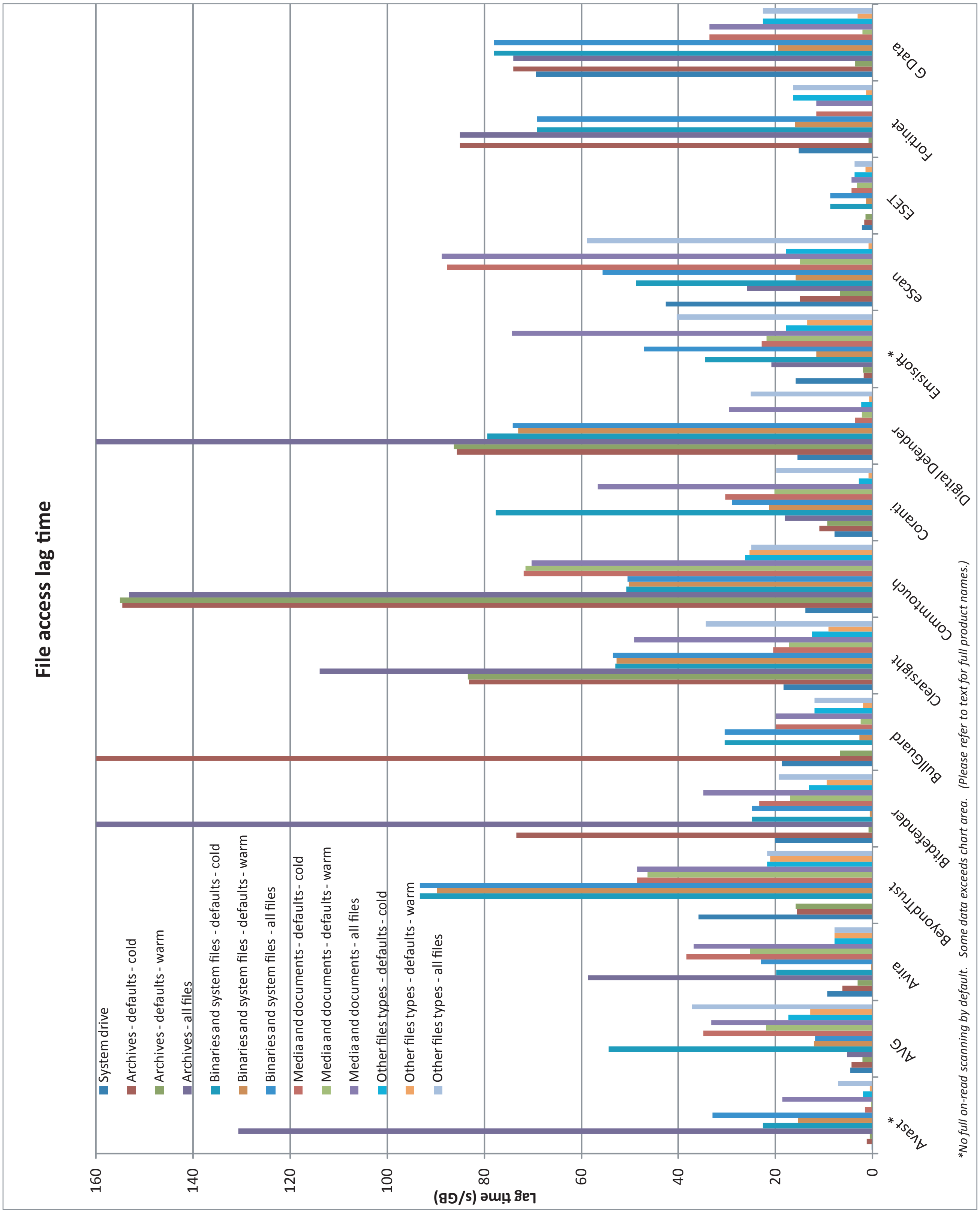
ItW Std	100.00%	**ItW Std (o/a)**	100.00%
ItW Extd	100.00%	**ItW Extd (o/a)**	100.00%
False positives	1	**Stability**	Stable



Ikarus recently tweaked the name of its product, but little else appears to have changed. As usual, the submission was provided as a full ISO image for an installation CD, doubtless including much else besides the basic product but still fairly compact at just over 200MB. Updates are provided separately for offline use, weighing in at 89MB. Set-up has a fair number of steps and much of the fairly lengthy time it takes is down to the installation of the .NET framework – those who already have this in place will of course enjoy a faster set-up time. On completion of the job a message reported errors in the network which prevented updating, but Internet access seemed to be fine and re-running the update task once the install was complete proved problem-free – it did take some time however, with the whole install process averaging more than ten minutes.

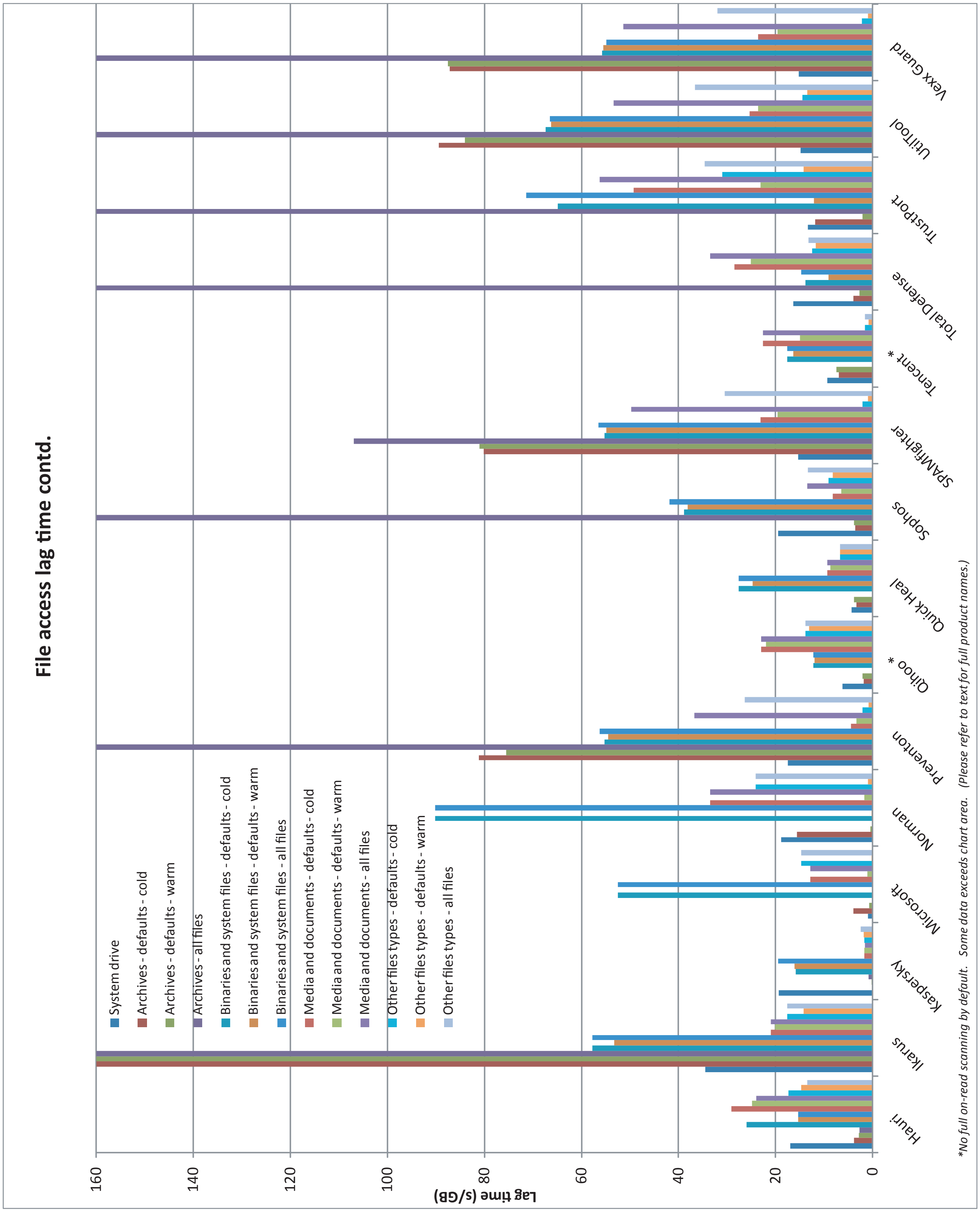
The product interface, in the .NET style, is sparse and simple. It is a little slow to respond at times but reasonably stable; it does become very laggy when under heavy pressure though. Configuration is a little more than minimal, but fairly easy to navigate, and logging is thorough and readable. Scanning speeds were not great – better in the sets of media and miscellaneous files than elsewhere – while lag times were distinctly heavy. Resource use was also high – particularly CPU use, which was off the chart – but our set of tasks didn't take too long to get through.

Detection rates were superb, dropping off only very slightly in the last few days of the response tests and remaining above 90% even in the proactive part of the RAP sets – a remarkable achievement this month. As has so often been the case in the past though, this stellar detection is counterbalanced by a tendency to false alarm, and a single item in the clean sets, again from *HP*, was flagged as a



*No full on-read scanning by default. Some data exceeds chart area. (Please refer to text for full product names.)

File access lag time contd.



*No full on-read scanning by default. Some data exceeds chart area. (Please refer to text for full product names.)

trojan. This was enough to deny *Ikarus* a VB100 award despite good coverage of the WildList sets. *Ikarus*'s luck remains highly varied, with two passes and three fails in the last six tests; three passes and six fails in the last two years. Stability this month was decent, with just some minor wobbliness in the GUI under heavy pressure, earning the product a 'stable' rating.

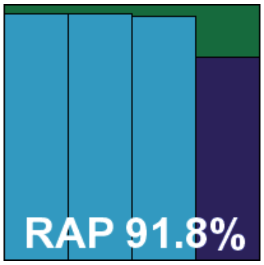
Kaspersky Endpoint Security 8 for Windows

Main version: 8.1.0.831

Update versions: 8.1.0.831 (a)

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

vb 100 VIRUS Oct 2012 virusbtn.com



Kaspersky's business solution was provided this month as a sizeable 319MB install package, with updates, in the form of a mirror of the company's update servers, measuring close to 300MB but including much more than required for this product alone. Set-up followed standard lines and seemed to run fairly speedily, although at one point it did worry us slightly by vanishing for some time, with nothing to indicate any kind of activity for close to 30 seconds. After this the final stages zipped through very quickly, but the install was on the slow side. Updates were also slow, taking more than six minutes in every run, and in each case a reboot was requested rather quietly, so that only the more observant of users would be likely to notice it.

The interface is glossy and modern, with a quirky take on buttons and links in places, but it is reasonably simple to find one's way around and provides a superb degree of fine-tuning. It also seemed very stable under pressure. On one occasion an on-access job produced odd results with a number of misses, but re-running the same task moments later showed perfect coverage and the issue could not be reproduced. Scanning speeds were a little slow initially and blindingly fast in the warm runs, with very light overheads. Resource use was a little high, but our set of tasks got through in good time.

Detection was solid, with good scores across the board, and with no problems to report in the certification sets a VB100 award is comfortably earned. That leaves *Kaspersky* on five passes and a single fail in the last six tests; eight passes and three fails in the last two years. With only a single, non-reproducible issue observed, a 'stable' rating is earned.

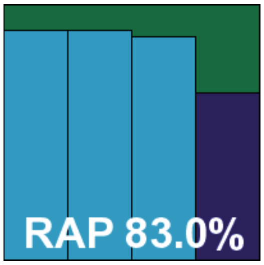
Microsoft System Center 2012 Endpoint Protection

Main version: 2.2.903.0

Update versions: 1.1.8601.0/1.131.1805.0, 1.1.8704.0/1.135.1150.0, 1.135.1404.0, 1.135.1568.0

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

vb 100 VIRUS Oct 2012 virusbtn.com



Microsoft's business product is another that has undergone a rebranding of late – once again with little difference in the overall user experience. The package provided was an 83MB zip archive, containing the compact 17MB main installer and an offline update bundle. Set-up was fast and simple, with minimal interaction required; updates averaged around a minute, taking the total install time to not much more than a minute and a half.

The interface is simple and mostly straightforward, although a little wordy in places. It was generally responsive, although during one of the RAP jobs we did fear it had frozen up entirely – we later found it was simply taking its time. Later on, though, we hit a more serious problem when a scan of one of the Response sets which had been set to run overnight was found in the morning to have got nowhere, a message simply stating that the scan could not be run. On rebooting the system prior to another attempt, we were shown a message indicating that the main service had stopped running unexpectedly. The reboot seemed to clear things up adequately though.

Speeds were no more than OK, but overheads were pleasingly light, with low RAM use, CPU use a little below average for the month, and our set of tasks barely affected by the protection. Detection scores were not bad, dropping rather sharply into the proactive part of the RAP sets, but remaining impressively stable through the Response sets. The core sets presented no difficulties, and a VB100 award is well deserved; our test history for *Microsoft*'s business line shows rather sporadic entries but solid performances,

Response tests	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
Avast	94.02%	87.44%	89.63%	86.11%	76.28%	71.30%	75.95%	82.96%
AVG	99.44%	97.76%	99.09%	98.25%	99.37%	98.81%	95.83%	98.36%
Avira	99.69%	99.30%	99.55%	99.58%	99.58%	99.42%	99.27%	99.49%
BeyondTrust	77.21%	83.36%	84.86%	81.23%	59.41%	83.82%	66.75%	76.66%
Bitdefender	99.16%	98.38%	98.51%	98.59%	97.93%	97.45%	96.13%	98.02%
BullGuard	99.17%	98.42%	98.49%	98.62%	97.97%	97.55%	95.61%	97.97%
Clearsight	92.54%	92.31%	87.06%	82.06%	79.08%	69.07%	52.18%	79.18%
Commtouch	97.76%	98.75%	99.15%	99.15%	99.16%	93.88%	86.96%	96.40%
Coranti	99.39%	98.95%	99.47%	99.55%	97.97%	98.25%	96.54%	98.59%
Digital Defender	92.54%	92.31%	87.06%	82.06%	79.08%	69.07%	50.60%	78.96%
Emsisoft	99.47%	99.09%	99.55%	63.79%	95.77%	98.84%	97.72%	93.46%
eScan	98.85%	98.85%	98.50%	98.80%	97.63%	97.19%	95.54%	97.91%
ESET	94.14%	95.37%	94.86%	97.23%	92.95%	95.70%	96.63%	95.27%
Fortinet	99.11%	98.06%	98.09%	98.84%	98.73%	96.96%	86.32%	96.59%
G Data	99.52%	99.36%	99.71%	99.76%	99.26%	99.11%	99.41%	99.45%
Hauri	81.77%	80.09%	83.72%	83.55%	73.49%	62.70%	67.29%	76.09%
Ikarus	99.80%	99.84%	99.71%	99.65%	99.08%	98.90%	98.67%	99.38%
Kaspersky	97.13%	96.58%	97.35%	98.06%	97.63%	94.75%	96.43%	96.85%
Microsoft	90.17%	95.26%	93.11%	92.94%	93.54%	90.82%	92.05%	92.56%
Norman	94.85%	89.26%	95.12%	87.96%	62.58%	85.29%	69.19%	83.46%
Preventon	92.54%	92.31%	87.06%	82.06%	79.08%	69.07%	50.60%	78.96%
Qihoo	99.32%	98.80%	98.68%	98.60%	97.40%	97.41%	96.34%	98.08%
Quick Heal	70.46%	75.44%	83.51%	76.62%	74.64%	49.08%	71.74%	71.64%
Sophos	97.64%	97.86%	98.15%	98.23%	98.19%	88.29%	88.01%	95.20%
SPAMfighter	92.54%	92.31%	87.06%	82.06%	79.08%	69.07%	50.60%	78.96%
Tencent	90.15%	94.28%	97.63%	88.33%	83.42%	95.25%	91.41%	91.49%
Total Defense	50.54%	56.96%	60.17%	48.26%	43.55%	57.50%	51.70%	52.67%
TrustPort	99.84%	99.77%	99.89%	99.92%	99.93%	99.48%	98.77%	99.66%
UtilTool	92.55%	92.39%	87.07%	82.12%	79.92%	71.12%	53.46%	79.80%
Vexx Guard	92.55%	92.39%	87.07%	82.12%	79.91%	70.01%	53.46%	79.64%

(Please refer to text for full product names.)

with two passes from two attempts in the last six tests; five from five in the last two years. A few oddities were noted this month, but a ‘stable’ rating is still merited.

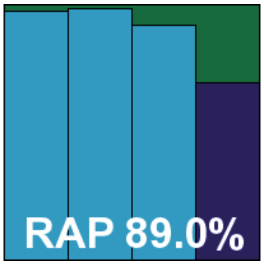
Norman Endpoint Protection

Main version: 9.00

Update versions: 6.08.06

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

vb 100 VIRUS virusbtn.com Oct 2012



Norman’s scores have improved significantly over the last six months, and we came into this month’s test hoping to see more of the same. The package submitted for testing was a 253MB executable, and as usual it seemed to run through its business impressively quickly. Once all appeared to be done with however, the product interface and system tray icon were unavailable or incomplete for some time – there was clearly much more going on in the background. Judging the actual time taken for installation was thus rather tricky, but on most runs it seemed to be at least three minutes before everything was fully functional. Several more minutes would then be required for initial updates.

The interface is displayed by a browser, and under the default security settings in *Windows Server 2003*, a number of warnings have to be dealt with before local content can be displayed, including acceptance of exceptions to security rules. With this done, a number of scripting errors were alerted on – a total of seven each time we opened the interface – and once up it took some time to fully display, leaving several areas worryingly blank to start with. The layout is reasonable but can be tricky to handle as it lacks the flexibility of a proper interface. The lack of warnings when navigating away from a page without having saved any changes made to the configuration have confused things for us in the past. This month we noted an oddity in the logging system, with on-access detections appearing fleetingly when the real-time log is opened, but vanishing before anything can be read properly.

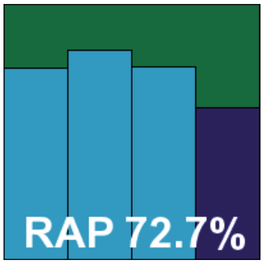
Otherwise things moved along nicely, with long, slow scans of our speed sets, particularly the archive set, but lag times not looking bad at all thanks to some smart improvements in the warm runs. RAM use was low, CPU use a little high, and our set of tasks ran through quickly. Detection rates were solid in the earlier part of the RAP sets, dropping off fairly sharply into the proactive week, and also started well in the Response sets, again tailing away quite severely into the more recent sets. The core sets were dealt with well though, and a VB100 award is earned, keeping *Norman* on a very respectable six passes in the last six tests; 11 passes and a single fail in the last two years. Stability was rated ‘fair’ thanks to a number of mostly minor problems with the interface and logging.

Preventon Antivirus for Server

Main version: 4.3.91

Update versions: 15.0.147, 15.0.188, 15.0.192, 15.0.194

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Stable



Progenitor of the usual cluster of participants, a few of *Preventon*’s offspring have already been discussed this month, and attentive readers will be able to predict how *Preventon* itself fared. Installation was highlighted by issues with the updating display, and also on one occasion by the product switching from English into German after the initial update. The interface was mostly reliable after install, and speeds were not too bad. Overheads were rather high, resource use a little high, particularly for CPU cycle use, and impact on our set of tasks a tad high too.

Detection was rather mediocre, with fairly steep downward slopes through both the RAP and Response sets, and although a clean sheet was managed in the false positive tests the WildList was not well handled, meaning no VB100 award for *Preventon* this month. The vendor’s test history is mostly decent, with three passes and now a single fail in the last six tests; seven passes and two fails from nine entries in the last two years. How things go in the future will depend greatly on how well the new engine developers can handle the transition. Stability was also a little shaken this month by some oddities that occurred during install and update, with a score only just within the ‘stable’ range.

Qihoo 360 Antivirus

Main version: 3.0.0.3051

Update versions: NA

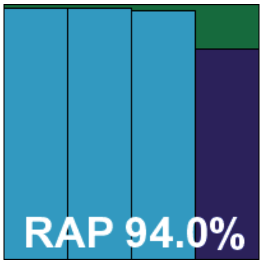
Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities - time increase
Avast	4.56%	4.20%	46.39%	14.19%
AVG	1.63%	2.76%	2.28%	4.89%
Avira	2.08%	2.63%	26.25%	5.30%
BeyondTrust	5.85%	5.34%	115.41%	7.22%
Bitdefender	2.84%	3.93%	24.91%	11.53%
BullGuard	7.60%	7.71%	89.03%	15.41%
Clearsight	10.34%	10.68%	67.51%	15.28%
Commtouch	2.20%	2.44%	149.49%	207.60%
Coranti	16.67%	14.92%	62.99%	10.68%
Digital Defender	6.16%	6.35%	58.54%	9.94%
Emsisoft	0.41%	2.61%	5.08%	18.65%
eScan	0.52%	2.40%	9.94%	7.68%
ESET	3.89%	3.85%	38.22%	5.30%
Fortinet	6.21%	4.35%	55.20%	14.86%
G Data	43.25%	45.00%	49.93%	30.44%
Hauri	8.33%	8.95%	4.55%	38.06%
Ikarus	7.49%	8.16%	105.93%	14.58%
Kaspersky	11.19%	12.06%	77.91%	8.67%
Microsoft	3.30%	3.24%	44.02%	4.38%
Norman	5.32%	4.94%	57.26%	2.99%
Preventon	8.05%	8.38%	78.65%	10.68%
Qihoo	0.96%	1.74%	0.41%	0.75%
Quick Heal	11.43%	12.35%	31.79%	4.01%
Sophos	7.87%	8.14%	57.09%	14.28%
SPAMfighter	6.21%	6.51%	70.35%	9.12%
Tencent	6.02%	5.87%	18.16%	6.10%
Total Defense	16.82%	16.97%	45.73%	5.84%
TrustPort	4.27%	5.68%	18.80%	8.93%
UtilTool	5.24%	5.79%	53.30%	9.92%
Vexx Guard	9.71%	10.14%	73.14%	10.94%

(Please refer to text for full product names.)

Qihoo 360 Antivirus contd.

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

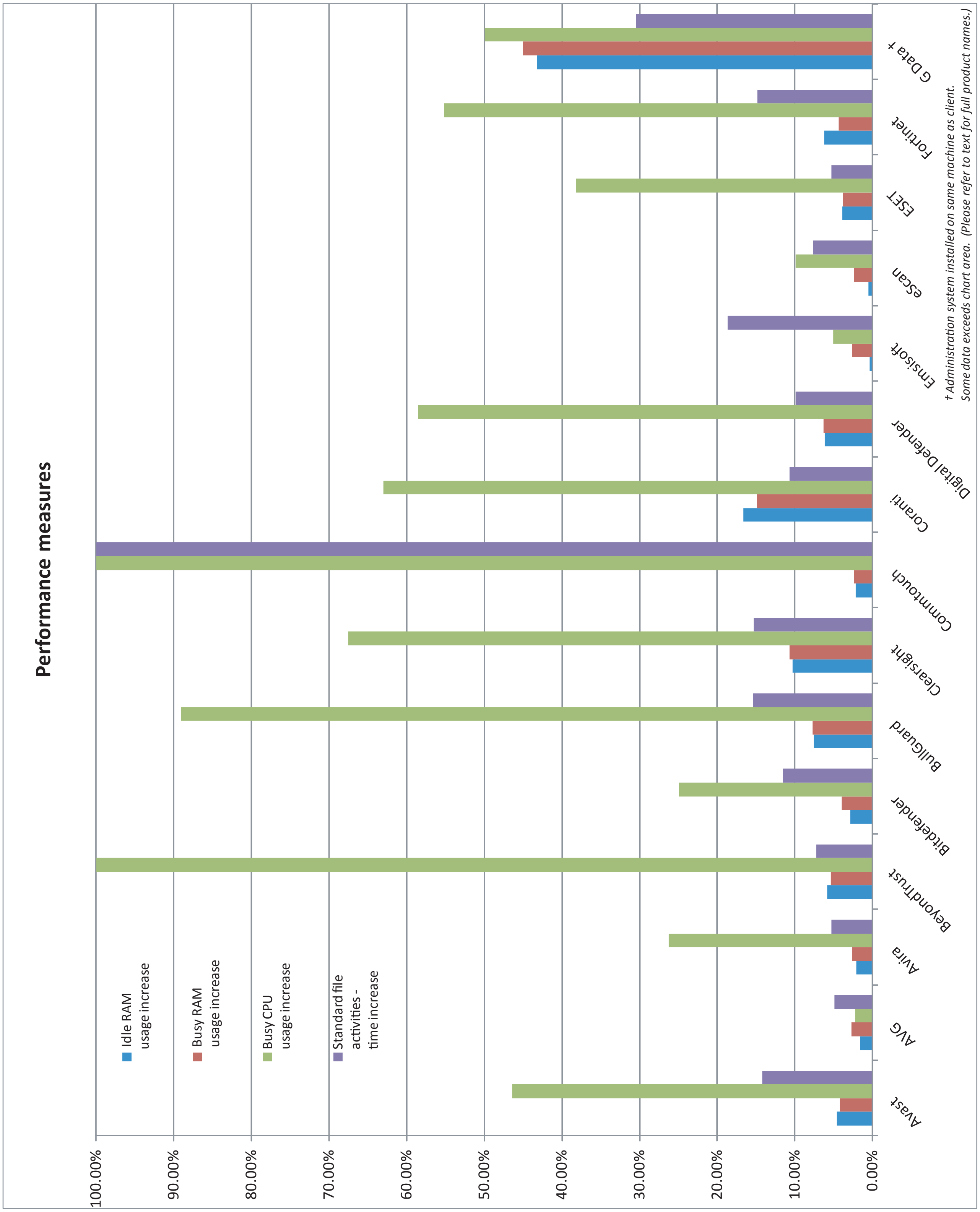
vb 100 VIRUS virusbtn.com Oct 2012



Qihoo's *360* is another product that uses the *Bitdefender* engine. We noted recently that it also offers access to the *Avira* engine, but as this is not enabled by default we have never looked at its impact in our tests. In the past, the product's performance has generally been decent, although we have encountered issues with updating and with the distinctly unusual approach to what can only very loosely be described as real-time protection. The current version came as a 134MB executable, which ran through rapidly with minimal interaction. Installation seemed to be complete in well under a minute, but once again updates were less than reliable, with several attempts returning a rather unhelpful 'failed' message, while others claimed success but made no changes to the reported version information. On most runs we did eventually get things into what appeared to be an updated state, with more than a little effort in most cases.

The interface is fairly simple and easy to operate, with a reasonable level of control, and in general it seemed to run reliably. As noted repeatedly in the past, on-read protection is more than a little quirky, apparently observing that files have been accessed and adding them to a queue to be checked; some time later (several hours if a heavy barrage of detections is forced), a message appears informing the user that a threat has been detected and access to it has been blocked – but this often seems to be rather a case of shutting the stable door long after the horse has made off with your sensitive data. Fortunately, as far as we can tell, on-execution checks are a little more rigorous.

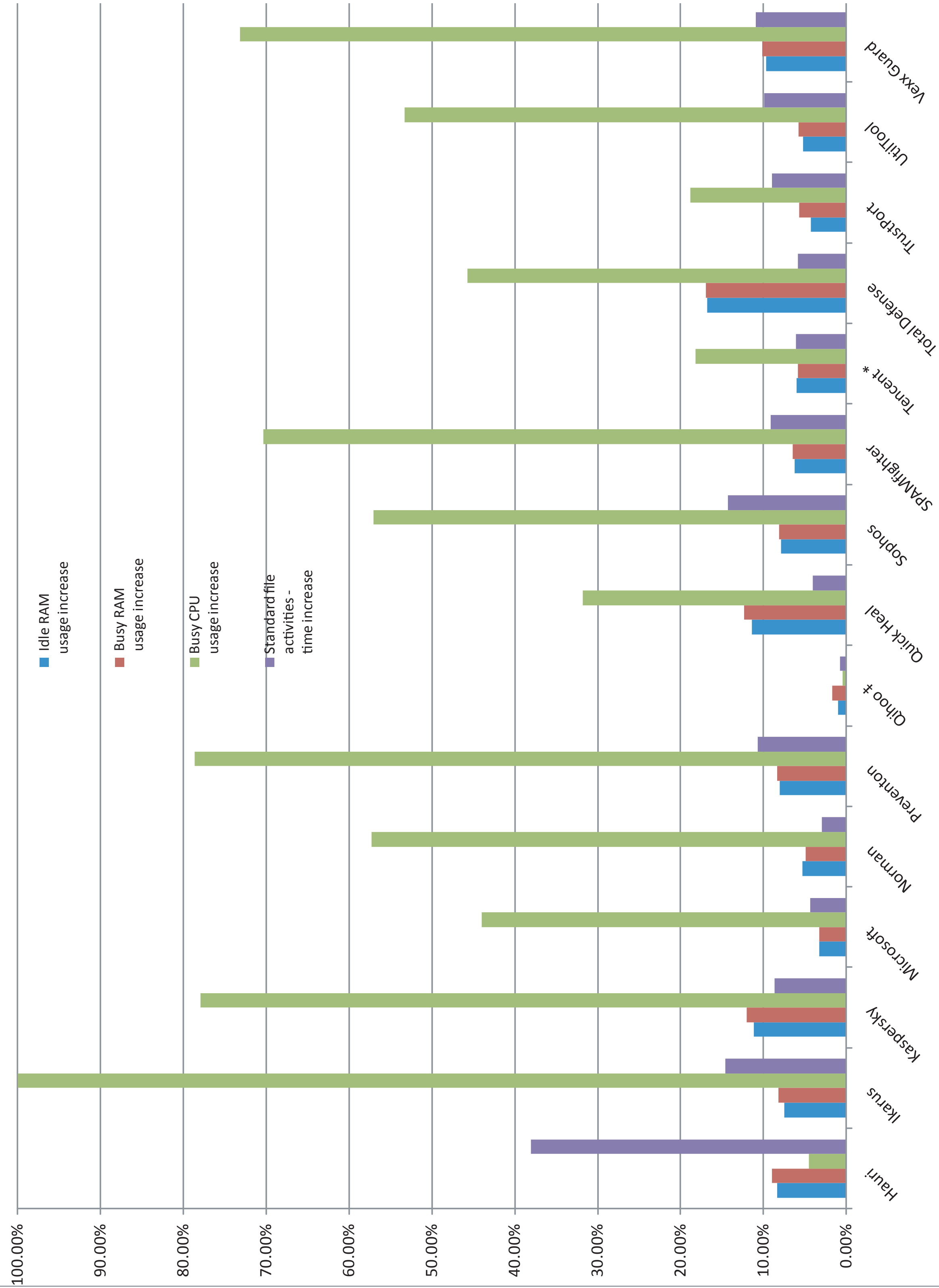
Scanning speeds were around average, with overheads heavier than might be expected given the minimal intrusion. Resource use was barely noticeable though, and our set of tasks apparently bypassed the notice of the product entirely. Detection rates were excellent throughout, confirming that our hard work with the updates had paid off, and the core sets were well dealt with, earning *Qihoo* a VB100 award. That puts the vendor on two passes and two fails from four entries in the last six tests; five passes and two fails in the last two years. Ignoring the real-time oddness as a feature



Performance measures

† Administration system installed on same machine as client.
Some data exceeds chart area. (Please refer to text for full product names.)

Performance measures contd.



*No on-read scanning active by default. ‡Real-time scanning not fully real time. Some data exceeds chart area. (Please refer to text for full product names.)

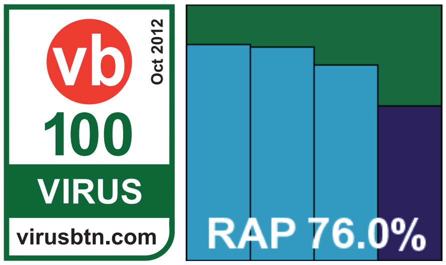
rather than a bug, there were a few little wobbles mainly in the updater component, and a ‘stable’ rating is earned.

Quick Heal AntiVirus – Server Edition

Main version: 13.00 (6.0.0.4)

Update versions: NA

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



One of our long-time regulars, *Quick Heal* has hit a bit of an unlucky patch of late. The vendor’s latest version for servers was provided as a 257MB installer, which started with some initial preparation and a scan of system memory, before following a more standard path to complete the set-up in under a minute. Updates downloaded rapidly but took some time to complete installation, making for a total install time of around four minutes.

The interface is glossy on the surface but crisp and business-like underneath, with a good level of control offered. One thing lacking which we would like to see is an option to export on-access logs to plain text. Things were mostly easy to find and seemed to run solidly under pressure.

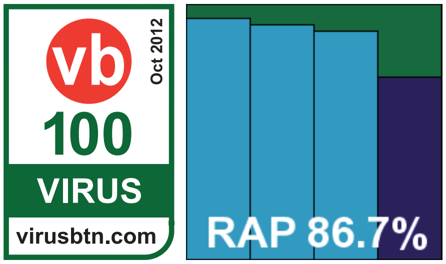
Scanning speeds were good and overheads light, with resource use well below average and an impressive time taken to complete our set of tasks. Detection rates were less than stellar, dropping steadily in the RAP sets and rather unpredictable in the Response sets. The core sets were handled properly though, with no issues to report, and a VB100 award is earned. No stability issues were observed, and *Quick Heal* joins the elite ranks of those rated ‘solid’ this month.

Sophos Endpoint Security and Control

Main version: 10.0

Update versions: 10.0.7/3.34.0/4.80G, 10.0.8/3.35.1/4.81G

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



Sophos recently suffered one of those periodic major false positive disasters which make news headlines even outside of the technical press – and to which all big security vendors seem prone from time to time. Luckily for *Sophos*, the incident occurred just outside of this month’s VB100 testing cycle. The company provided its submission as a 98MB installer with updates of only 7MB; set-up dished out no surprises and completed in around two minutes, with updates adding another minute or so on average.

The product GUI is clear and simple to operate, with decent main controls and a huge amount of fine-tuning provided behind a warning not to meddle if you don’t know what you’re doing. Operation was steady and reliable, with no issues noted.

Scanning speeds were pretty good in most areas, apart from archives which are analysed in some depth by default. On-access lag times were fairly light, and in this case extra light on archives, which are ignored by default in this mode, as are files with non-threatening extensions. With settings turned up things do get a little slower, but not significantly so. Resource use was around average for the month, and the time taken to get through our set of tasks was quite decent.

Detection was solid in the Response sets, although it tailed off noticeably in the most recent few days, and the RAP scores showed a similar pattern of starting high but dropping quite a bit into the proactive week. With the vendor’s false positive incident hitting just days after testing had finished, the core sets presented no problems, and a VB100 award is earned. That puts *Sophos* on four passes and two fails in the last six tests; its longer-term test history is much better with ten passes and two fails. With no stability issues observed, *Sophos* earns a ‘solid’ rating this month.

SPAMfighter VIRUSfighter PRO

Main version: 7.1.258

Update versions: NA

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Fair

Using the *Preventon* SDK to the engine now referred to as *Agnitum*’s (formerly *VirusBuster*), *SPAMfighter* has made

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Avast	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	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/√	√
BeyondTrust	OD	X	1	1	1	1	1	1	8	2	X	√
	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/√
BullGuard	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	2	2	1	1	2	2	2	1	2	2	√
Clearsight	OD	2	2	X	X	2	X	2	1	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Commtouch	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2	2	2	2	2	√	2	1	2	2	√
Coranti	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	X	X	√	X	X	X	1	X/1	X/√
Digital Defender	OD	2	2	X	X	2	X	2	1	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Emsisoft	OD	√	√	X	X	√	√	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
eScan	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/9	8	8	X/√	1/√	X/√	X/8	X/√	X/√	√
ESET	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Fortinet	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√	√	√
G Data	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√

Key:

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

X - No detection of EICAR test file

X/√ - default settings/all files

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

* Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names.)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
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/√	X/√
Microsoft	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	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	1	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Qihoo	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X	X	1	1	1	X	X	X	1	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	√
Sophos	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	5	5	5	5	5	5	5	5	5	√
SPAMfighter	OD	2	2	X	X	2	X	2	1	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Tencent	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	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	√
TrustPort	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
UtilTool	OD	2	2	X	X	2	X	2	1	2	2	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Vexx Guard	OD	2	2	X	X	2	X	2	1	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

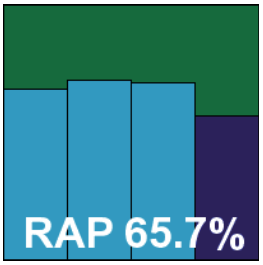
X/√ - default settings/all files

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

* Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names.)

a few more changes to the look and feel of its solution than most related offerings. The 85MB installer runs quickly and simply, although somewhat unusually it asks for a user email address. The GUI is fairly clear with a decent basic level of controls.



Scanning speeds were on the slow side, with file access lags fairly heavy. RAM use was low but CPU use high, while our set of activities didn't take too long to get through. Detection was not great, with the expected fairly sizeable batch of misses in the WildList denying *SPAMfighter* certification this month. As in most tests, we observed some serious instability in the interface under any kind of pressure – detecting more than a few dozen samples in a row sends it into something of a tizzy, flickering, juddering and eventually freezing completely. As this prevents access to some other windows, including the one requesting reasons for rebooting presented in this server platform, rebooting to cure the issues was often fairly tricky – but always effective. Hopefully such issues would not affect too many real-world users, but on server platforms this kind of scenario is quite possible.

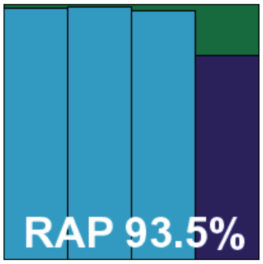
The product's test history is decent, with three passes and now a single fail in the last six tests; seven passes and two fails in the last two years. The issues encountered were fairly inconvenient, but only occurred under heavy pressure, and the stability score falls into the 'fair' range.

Tencent PC Manager

Main version: 6.6.2284.201

Update versions: NA

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



Tencent returns for its third consecutive test, giving the lab team a change from the everyday with its Chinese-only interface. Installation from the 117MB package submitted was something of a mystery tour, with several dialogs to click through without much idea of what they were asking. The whole business was completed in under a minute though, with no need to reboot (as far as we could tell). Updates mostly ran to around two minutes for the initial run, although on one occasion they froze at around 2% complete, sitting there for over an hour before we noticed nothing was happening. Rebooting and re-running the tasks was more successful however, with no repeat of the issue.

Scanning speeds were rather slow, and the overhead measures are not comparable with others as on-read scanning appears to be unavailable. Resource use and impact on our set of tasks was low, but again the lack of the full real-time protection provided by most other products affects this measure greatly. Detection rates from the *Avira* engine underlying the anti-malware component of what appears to be a multi-part suite were good, but perhaps not quite as excellent as we would expect, with solid RAP scores but Response scores some way below those scored by *Avira*'s own solution – hinting perhaps that updates either lag a little behind the times or were not fully successful in every run.

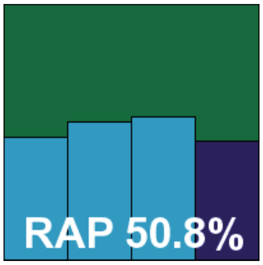
Nevertheless, the core sets were well covered with no misses in the WildList and no false alarms in the clean sets, and *Tencent* earns its third VB100 award on its third attempt. Stability was decent, with just a single issue occurring during one of the updates, thus earning a 'stable' rating.

Total Defense Inc. Total Defense r12

Main version: 12.0.0.833

Update versions: 12.0.0.832/1.6.0.1884/5935.0.0.0, 5978.0.0.0, 5981.0.0.0, 5987.0.0.0

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



The business offering from *Total Defense* was installed as usual from a full DVD ISO image measuring over 3GB, but this of course includes far more than the client solution tested here. Updating could apparently only be provided online on the deadline day, despite options in the product interface clearly offering the choice to update from a local file. Set-up is slowed considerably by the need to have the .NET framework in place, which takes around four to five minutes to set up if not already present, and also requires a swathe of personal data to be filled in. However, once this

Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Avast	VIRUS 100	97.14%	96.87%	97.28%	97.10%	79.38%	92.67%
AVG	VIRUS 100	96.96%	97.71%	95.95%	96.87%	71.95%	90.64%
Avira	VIRUS 100	99.13%	99.27%	97.49%	98.63%	80.15%	94.01%
BeyondTrust	VIRUS 100	97.54%	98.55%	82.72%	92.94%	71.68%	87.63%
Bitdefender	VIRUS 100	98.11%	98.03%	97.11%	97.75%	82.37%	93.91%
BullGuard	VIRUS 100	98.19%	98.07%	97.37%	97.88%	82.85%	94.12%
Clearsight		74.93%	81.64%	75.13%	77.24%	59.08%	72.70%
Commtouch		67.78%	74.07%	68.26%	70.04%	55.14%	66.31%
Coranti		98.85%	98.78%	98.00%	98.54%	83.70%	94.83%
Digital Defender		74.93%	81.64%	75.13%	77.24%	59.08%	72.70%
Emsisoft		70.10%	61.15%	97.40%	76.22%	62.92%	72.89%
eScan	VIRUS 100	98.07%	97.95%	95.51%	97.18%	81.01%	93.13%
ESET	VIRUS 100	94.39%	86.19%	93.43%	91.34%	79.54%	88.39%
Fortinet	VIRUS 100	97.62%	98.16%	98.37%	98.05%	92.17%	96.58%
G Data	VIRUS 100	99.54%	99.47%	99.27%	99.43%	86.43%	96.18%
Hauri	VIRUS 100	96.87%	98.07%	97.15%	97.36%	82.42%	93.63%
Ikarus		99.38%	99.68%	98.43%	99.16%	90.25%	96.94%
Kaspersky	VIRUS 100	96.42%	96.26%	95.30%	95.99%	79.33%	91.83%
Microsoft	VIRUS 100	90.00%	89.58%	87.23%	88.94%	65.32%	83.03%
Norman	VIRUS 100	97.09%	98.05%	91.71%	95.62%	69.28%	89.03%
Preventon		74.93%	81.64%	75.12%	77.23%	59.08%	72.69%
Qihoo	VIRUS 100	98.22%	98.09%	97.17%	97.83%	82.44%	93.98%
Quick Heal	VIRUS 100	84.45%	83.03%	76.18%	81.22%	60.47%	76.03%
Sophos	VIRUS 100	94.04%	91.81%	89.40%	91.75%	71.50%	86.69%
SPAMfighter		67.00%	70.37%	69.48%	68.95%	56.04%	65.72%
Tencent	VIRUS 100	98.09%	98.51%	97.46%	98.02%	79.90%	93.49%
Total Defense	VIRUS 100	47.93%	53.57%	55.71%	52.41%	46.16%	50.84%
TrustPort	VIRUS 100	99.62%	99.57%	99.26%	99.49%	85.26%	95.93%
UtilTool		74.93%	81.64%	75.13%	77.24%	59.08%	72.70%
Vexx Guard		74.93%	81.64%	75.13%	77.24%	59.08%	72.70%

(Please refer to text for full product names.)

was out of the way the set-up process was fairly speedy, with updates also fast, taking under a minute on each run. Our overall install time of close to ten minutes includes the .NET stage – without this it would more or less be halved. On completion of the installation a reboot is required, and another was requested after most updates. On one occasion, after this second update the interface could not be accessed, with no response from the system tray icon either, for well over five minutes. A third reboot was blocked by the 'catm.exe' process, which had to be forcibly closed, but after this restart things went smoothly once again.

The product interface is simple and clear, with reasonable if not comprehensive controls, and it operated well under pressure for the most part. Scanning speeds were very zippy even at first attempt, and even faster in the warm runs, with overheads pretty light, at least until settings were turned up high. RAM use was fairly high, but CPU use was below average and our set of tasks tripped through in excellent time.

Detection was pretty disastrous, dropping below 50% in some of the Response sets and even one of the reactive weeks of the RAP sets. Fortunately this poor showing did not extend to the WildList, which was well covered, and with no false alarms either *Total Defense* earns a VB100 award. With some minor interface problems observed, the product's stability score falls just inside the 'stable' range.

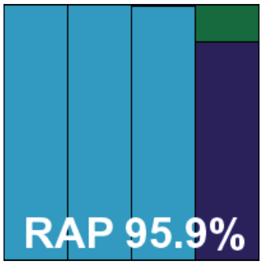
TrustPort Antivirus 2013

Main version: 13.0.2.5069

Update versions: 13.0.4.5077

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

vb 100 VIRUS virusbtn.com Oct 2012



In the last test we noted that *TrustPort*'s offering seemed to have been reduced to a single engine, but things were back to normal this time, with both *AVG* and *Bitdefender* on board. The installer submitted weighed in at 216MB, including all required data for both engines, and ran through fairly speedily, including what appeared to be an update in a total runtime of under a minute. A reboot was required at the end, after which the system took some time to wake up, at which point it was clear that further updating was needed. This varied in time from two to ten minutes, with total data of around 80MB to download.

The interface remains a little unusual and can be tricky to find one's way around, but mostly makes sense after a little practice and exploration; configuration is limited in the main areas, but fairly in-depth once the advanced control panel is discovered.

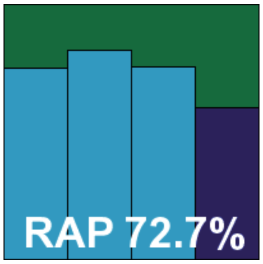
Scanning speeds were not very exciting, with overheads a little high, but use of resources was impressively low for a dual-engine solution, and our set of tasks got through in good time. Detection was uniformly excellent, with only the very latest day of the Response sets and the proactive part of the RAP test falling below 99%. The core sets were effortlessly brushed aside, and a VB100 award is easily achieved by *TrustPort*. Recovering from a recent rough patch, its test history now shows three passes and two fails in the last six tests; seven passes and two fails in the last two years. With the usual odd window behaviour observed several times during the test but no more serious issues, a 'stable' rating is earned.

UtilTool Server Antivirus

Main version: 3.1.46

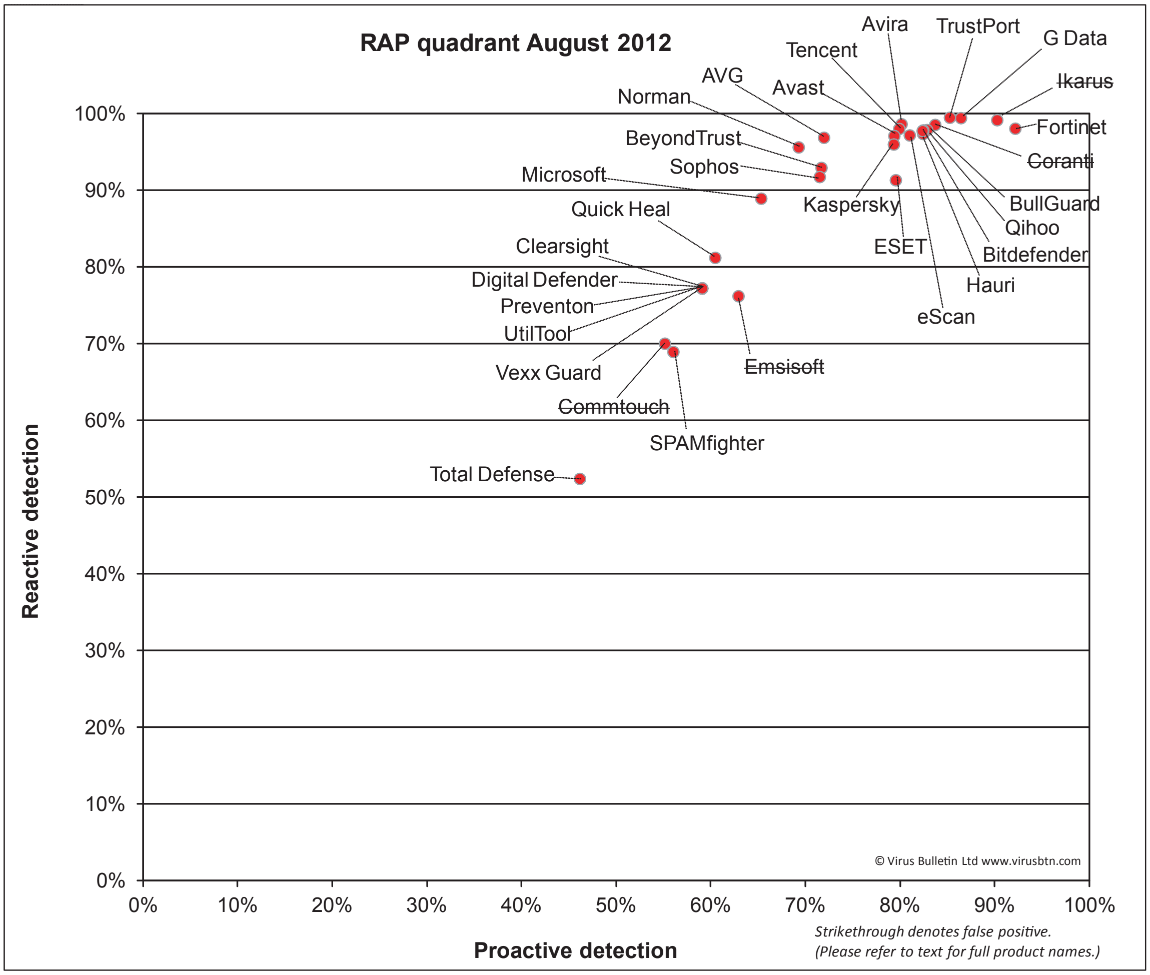
Update versions: 15.0.147, 15.0.188, 15.0.192, 15.0.194

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Fair



Another member of the *Preventon* family that has been plagued by problems this month, *UtilTool*'s chances of achieving a VB100 seemed slim. The 83MB installer ran through in good time and updates were fairly speedy. Once again, on completion the updates seemed to have made no difference – a reboot was not requested but seemed to be required to get the version details to catch up with reality. The interface is a newer version than the others tested this month, and has a few bugs of its own. For example, reboots did not work on first attempt, doing no more than shutting down the product interface – a second reboot was needed to actually restart the machine.

The interface remains fairly accessible though, providing a reasonable degree of control. Scanning speeds were not great but not too bad either, and overheads pretty high. RAM use was low, CPU use a little above average, but our set of activities was not badly affected at all. Detection was mediocre, with fairly dismal scores in the RAP sets, earlier parts of the Response tests not too bad but soon falling away, and as expected, the WildList was not well dealt with, meaning there is no VB100 award for *UtilTool* this month.



Strikethrough denotes false positive.
(Please refer to text for full product names.)

Our test history for the vendor stretches back just over a year, with two passes and two fails from four entries in the last six tests, one more pass to add to that from just over a year ago. Stability this month was hit by a few fairly minor problems, putting it in the 'fair' range.

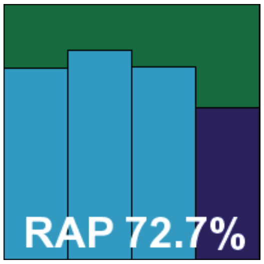
Vexx Guard Antivirus

Main version: 3.1.46

Update versions: 15.0.147, 15.0.188, 15.0.192, 15.0.194

ItW Std	98.25%	**ItW Std (o/a)**	98.07%
ItW Extd	95.89%	**ItW Extd (o/a)**	95.84%
False positives	0	**Stability**	Fair

The only new name on this month's list, *Vexx Guard* promised to liven things up but it quickly emerged as being yet another part of the ever-expanding *Preventon* clan, choosing a rather unlucky month to make its first appearance. The installer was larger than expected at 87MB, but that's where the surprises stopped – set-up was fast and simple, updates hit by the issue with the version information not updating properly, while reboots were again odd thanks to the implementation of the newer-style interface. Speeds were slowish, overheads heavy, RAM use OK but CPU use high, and the hit on our set of tasks not too bad.



Detection scores were disappointing, with low RAP scores, Response scores starting off passable but ending up poor, and the WildList showing a number of misses. There was thus no VB100 award for *Vexx Guard* on its first attempt. Stability was rated as 'fair' due to a number of small irritations.

UNTESTED PRODUCTS

In addition to those listed, a number of other products were also submitted, but found to be untestable for one reason or another – a severe shortage of precious testing time this month meant that we were perhaps quicker than usual to exclude products that did not behave well. Solutions from *BluePex*, *CMC*, *ESTsoft* and *RoboScan* were too unstable to produce usable results and were peremptorily dropped from the test. Several other solutions were submitted but found to be incompatible with the platform.

CONCLUSIONS

It was a rather quieter month than usual in terms of pure numbers of participants, but there was still more than plenty to keep us busy. The ratio of passes to fails was around normal, and although there were more issues with the WildList than usual these all came from a single family of solutions and can be put down to the difficult transition of engine development to a new company. Otherwise the main issue was, as usual, false alarms, with a large batch of software from major business developer *HP* causing the bulk of the problems this month.

Stability was a far bigger issue, with most products hit by at least some minor problems and a few showing some quite serious wobbles. On server platforms in particular security products must be exemplary in their reliability and trustworthiness – many admins consider problems caused by security products to be almost as serious as those caused by actual infections (an example of this was seen this month when one of the major vendors had a severe false positive issue that hit users worldwide). Developers clearly need to pay more attention to quality, in every sense of the word, before inflicting their products on the world, and our new stability rating system aims to encourage them to do just that.

This was a mature platform and developers should have had plenty of time to ensure their products run well on it; next up will be the all-new *Windows 8*, with the deadline for submissions set shortly before the full official release of the platform, so we can doubtless expect to see far more and far wilder issues. With the lab team hopefully back to full strength by then, we hope to claw back some time and publish the report on that test before the end of the year – judging by the difficulties encountered this month though, it looks like we could have our work cut out.

Technical details:

All products were tested on identical machines with *AMD Phenom II X2* 550 processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Microsoft Windows Server 2003 R2 SP2, 64-bit Enterprise Edition*. For the full testing methodology see http://www.virusbtn.com/vb100/about/methodology.xml.

VIRUS BULLETIN

Editor: Helen Martin

Technical Editor: Dr Morton Swimmer

Test Team Director: John Hawes

Anti-Spam Test Director: Martijn Grooten

Security Test Engineer: Simon Bates

Sales Executive: Allison Sketchley

Perl Developer: Tom Gracey

Consulting Editors:
Nick FitzGerald, *AVG, NZ*
Ian Whalley, *Google, USA*
Dr Richard Ford, *Florida Institute of Technology, USA*

SUBSCRIPTION RATES

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

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

Corporate rates include a licence for intranet publication.

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

- Comparative subscription: $100

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

Editorial enquiries, subscription enquiries, orders and payments:

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

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

Email: editorial@virusbtn.com 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.