



# virus

## BULLETIN

Covering the global threat landscape

## VB100 COMPARATIVE REVIEW ON SUSE LINUX ENTERPRISE SERVER 11

### INTRODUCTION

Our annual departure from the familiar *Windows* fare to the rather more exotic shores of the *Linux* world always has both upsides and downsides from a testing point of view. On the one hand, the market is significantly less crowded, and whereas a *Windows* desktop comparative would regularly feature 50 or more products, in *Linux* month it would be a surprise to see more than a dozen or so. Having fewer products to deal with should mean far less time is required to run through the testing programme, and the simplicity of automating tasks on the platform should also cut out a hefty chunk of hands-on time. On the other hand, products for *Linux* tend to be considerably less user-friendly than their *Windows* counterparts, with esoteric processes for installation and configuration noted frequently in previous *Linux* comparatives.

Starting late thanks to end-of-year holidays, products were taken in on the 19 December deadline, but testing work did not commence until well into January, with the bulk of it finished by early February.

In the past, a smaller field of competitors has often tended to go hand in hand with a higher VB100 pass rate. With only the most experienced of companies producing *Linux* products (or at least entering them in our comparatives), *Linux* tests tend to elicit fewer problems than usual in the certification areas. With only minimal expansion of our false positive sets this month, and relatively few tricky items existing in the WildList sets, the chances of seeing a 100% pass rate seemed fairly high – something which has not happened in at least the 40 comparatives run since testing duties fell into my hands in 2006, and as far as I can tell not at all in the history of the VB100. Of course, there was always the chance of a surprise upset, so as ever we knuckled down to testing with a mixture of anticipation and trepidation.

### PLATFORM AND TEST SETS

The latest version of *Novell's SUSE Linux Enterprise Server* platform, version 11 SP2, had a few surprises for us, having undergone a major kernel version change since its last appearance (already on v11) in the February 2010 comparative. Despite being almost a year old, this update promised to cause some havoc as, according to our contacts, the new kernel effectively broke the *dazuko/redirfs* approach (usually one of the most popular techniques) to providing on-access protection on *Linux*. In previous comparatives we have prepared and installed the *dazuko* module onto our systems from the off, but in this case we decided not to, and instead to see what options were provided by the products at submission time. So we went for a fairly bare install of the platform, which proved a relatively straightforward process. The GNOME desktop is installed by default – we left this as it was, expecting many products to provide some sort of interface. Setting up networking was a fairly routine task, with one system left running *Windows XP SP3* and connected to network shares on each test machine to act as a client for the on-access tests.

In a slight change to our traditional methodology, the WildList cut-off was set for the same date as the product submission deadline, 19 December. As our new approach means that testing against the WildList does not commence for some time after the submission deadline, and uses latest updates at the time of testing, it seemed reasonable to move the cut-off point forward a little to ensure we're keeping everyone well and truly on their toes. The November WildList, posted just a couple of days before our deadline, was thus used as the basis of our main certification sets.

The clean sets were little changed this month, with a relatively small number of new items added, mostly focusing on business software as befits the business leaning of this month's products. The RAP test sets were compiled

Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Suspicious
Avast*	99.88%	100.00%	99.88%	100.00%	0	0
AVG	100.00%	100.00%	100.00%	100.00%	0	0
Bitdefender	100.00%	100.00%	100.00%	100.00%	0	0
eScan	100.00%	100.00%	100.00%	100.00%	0	0
ESET	100.00%	100.00%	100.00%	100.00%	0	0
F-Secure	100.00%	100.00%	100.00%	100.00%	0	0
Kaspersky	100.00%	100.00%	100.00%	100.00%	0	2
Norman	100.00%	100.00%	100.00%	100.00%	0	0
Sophos	100.00%	100.00%	100.00%	100.00%	0	0

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

using the usual approach, with the final sets averaging 25,000 samples per week. The systems for building our Response sets were also unchanged, producing sets of around 2,500 samples per day.

The biggest changes were in our speed and performance sets, where a dedicated set of Linux files was built for speed measures. This contained the contents of several important sections of a standard Linux installation, including the /bin, /sbin, /etc and /lib directories. Some adjustments had to be made to our measurement processes to fit in with the systems, and this meant dropping our ‘standard activities’ measure for this test, which was unsuitable for the client/server approach. Otherwise things remained much the same as usual.

Most of the expected hard core of regulars turned up on the product deadline, with a couple of the larger companies – sporadic at best in their appearances of late – missing once again. The recent demise of VirusBuster meant that a couple of products we might usually expect to see were absent, and with a few more failing to appear – either thanks to issues with the platform or to internal company reorganizations – just nine products made the final cut, equalling the number seen in the last SUSE test three years ago.

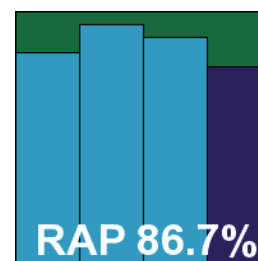
### Avast Software avast! For Linux/Unix

Main version: v3.2.1

Update versions: 121219-1, 130121-1, 130123-1, 130128-0

<b>ItW Std</b>	99.88%	<b>ItW Std (o/a)</b>	99.88%
<b>ItW Extd</b>	100.00%	<b>ItW Extd (o/a)</b>	100.00%
<b>False positives</b>	0	<b>Stability</b>	Solid

Avast’s developers were among the first to warn us of potential problems with the dazuko subsystem, but once we informed them that we were happy to change the kernel in use, everyone was happy. The submission was sent in as a 160MB archive, which contained everything needed to roll back the kernel and install the dazuko and redirfs modules, as well as the three RPM packages comprising the product itself. These were installed using the usual method, and everything else was found to be fairly standard, much to our satisfaction: configuration was adjusted using plain files in /etc, the location of the main executables was added to the search path, and ample man pages were provided describing the usage of the product in clear and simple terms. The only action required initially was the adjustment of one config file to point to a licence key, and then everything was up and running. The whole process, including the kernel adjustments and the reboot this necessitated, took only a couple of minutes. Updates were fairly speedy too, rarely taking more than 30 seconds or so.



The product ran without issues, proving just as stable to run as it was simple to operate. Scanning speeds were not bad – very fast indeed over our sets of media and miscellaneous files – with overheads showing a similar pattern. Memory use was low, but CPU use fairly high during busy times, not surprisingly. Detection was decent too – looking a little below par in some of our graphs, but this is entirely thanks to the quality of the opposition.

Product information	Install time (mins)	Reboot required	Third-party engine technology	Stability score	Stability rating
Avast	4	Y*		0	Solid
AVG	4.5	N		0	Solid
Bitdefender	3	N		1	Stable
eScan	4	N	Bitdefender	0	Solid
ESET	3	N		0	Solid
F-Secure	5	Y*	Bitdefender	6	Fair
Kaspersky	3	N		2	Stable
Norman	9	N		6	Fair
Sophos	3	N		0	Solid

0 = Solid  
 0.1 - 4.9 = Stable  
 5 - 14.9 = Fair  
 15 - 29.9 = Buggy  
 30+ = Flaky

\*Reboot required to change kernel version  
 Please refer to text for full product names.

Detection in the Response sets started very respectably and showed just a slight downward trend into the more recent days. The RAP sets were mostly well covered, but a rather sharp blip in the oldest week brought the average down somewhat.

The clean sets brought no surprises, and the WildList sets seemed to be well covered too, until the third of three test runs showed a loss of detection for a pair of samples in the standard set. The issue remained during further checks over the next few days, and was reported to the developers as a matter of urgency. Their feedback implied that the problem was thanks to the aged nature of the *Linux* product, lagging several cycles behind its *Windows* cousins (which were unlikely to be affected by the issue). Nevertheless, despite a generally strong showing *Avast* doesn't quite make the grade for VB100 certification, putting paid to our hopes for a clean sweep before we'd really got started. Our test history for *Avast* now shows one fail and five passes in the last six tests; ten passes and two fails in the last two years. Stability was fine this month once again, with a 'Solid' rating easily earned.

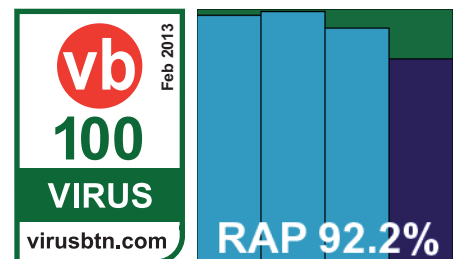
### AVG 2012 Linux Server Edition

Main version: 12.0.1795  
 Update versions: 2637/5465, 2639/5549, 2639/5553, 2639/5565

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

Clearly having received some recent attention from its developers, AVG's product managed to circumvent the problems with dazuko,

which remains supported where appropriate but on more recent kernels the fanotify system has been implemented. Installation of the product was fairly straightforward, with a single RPM of just over 100MB provided. This put everything in place nice and simply, but configuration was a little more complex than might be desirable, with a fairly lengthy syntax required to pass even fairly minor changes into the product. Figuring out the right wording was by no means straightforward, but was helped by some comprehensive man pages, and things were up and running in a decent amount of time. Initial updates seemed rather start-stop, taking over eight minutes to run through on the first attempt, but later runs were much smoother, all completing in under a minute.



Response tests	Day -7	Day -6	Day -5	Day -4	Day -3	Day -2	Day -1	Average
Avast	94.00%	93.83%	93.06%	93.62%	91.82%	91.35%	90.88%	92.65%
AVG	98.25%	98.21%	98.25%	98.12%	98.19%	97.95%	97.67%	98.09%
Bitdefender	97.08%	97.62%	97.24%	96.47%	93.47%	90.96%	89.34%	94.60%
eScan	96.94%	97.51%	97.20%	96.13%	93.24%	90.54%	88.78%	94.33%
ESET	93.61%	93.97%	93.15%	93.55%	93.63%	94.30%	93.86%	93.72%
F-Secure	96.72%	97.61%	97.52%	95.85%	93.36%	88.96%	90.76%	94.40%
Kaspersky	92.52%	91.36%	91.69%	93.07%	93.29%	93.74%	93.43%	92.73%
Norman	98.17%	97.98%	97.34%	97.27%	92.82%	94.39%	92.42%	95.77%
Sophos	97.40%	97.46%	97.30%	97.32%	96.70%	97.36%	95.97%	97.07%

Please refer to text for full product names.

Operation was generally fairly simple once the initial set-up had been completed, and things ran without problems. Scanning speeds were pretty good, and overheads not bad at all either, with a fair amount of RAM use but pretty low use of CPU cycles. Detection was excellent, with consistently high rates throughout our Response sets and RAP scores also starting very high indeed, tailing off rather more than most into the proactive week, but remaining pretty decent.

There were no problems in the core sets and a VB100 is comfortably earned by AVG; the vendor stands at one fail and five passes in the last six tests; two fails and ten passes in the last two years. This was another very smooth run, meriting a ‘Solid’ rating.

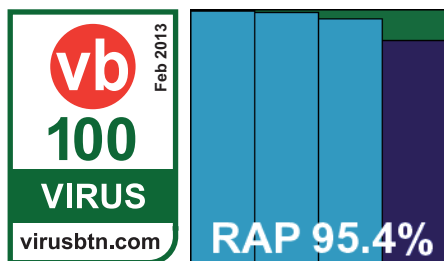
### Bitdefender Security for Samba Servers

Main version: 3.1.2

Update versions: N/A

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

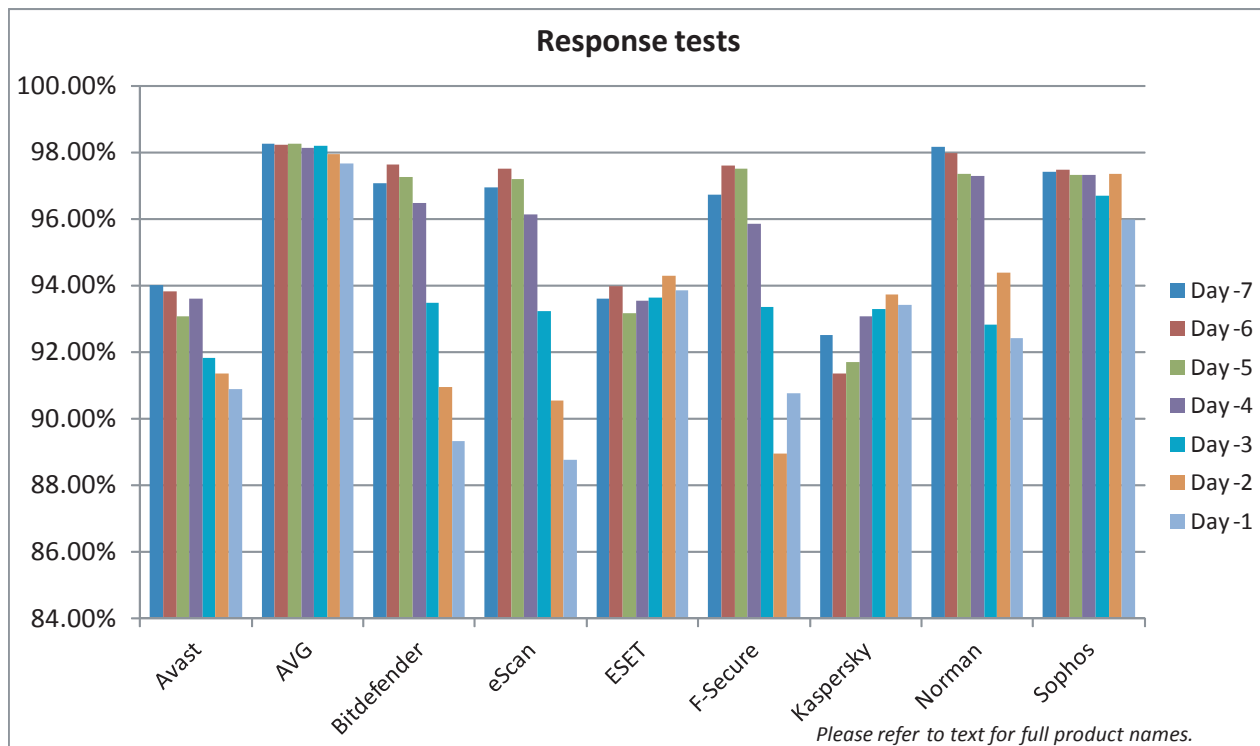
Bitdefender’s Samba-focused product also came as a single item, an executable-wrapped RPM installer which set things up simply and quickly, with minimal extra work needed to get



everything working nicely. Updates were swift too, but the design shies away from standard practice, using a complex system of commands passed into the main executable to make adjustments rather than the more common process of editing a plain-text configuration file. Nevertheless, with a little trial and error it soon became reasonably usable. Help was provided in the form of a set of man pages, but the set-up did not appear to have functioned properly so these were not discovered until late in the day, when rummaging through the product’s install directory for some ideas. The main executable was not added to the search path automatically, either.

On-access protection covers Samba shares only, by means of a VFS object pointed to by some tweaks to the Samba configuration file, which are put in place automatically during the set-up. Logging was a little verbose but clear enough and pretty reliable, while the basic syntax of the scanner was fairly straightforward once the schema had been worked out. Scanning speeds were on the slow side, and on-access overheads perhaps a little higher than some this month, with fairly high use of RAM but low CPU use.

Detection was superb though, continuing a recent string of excellent scores from Bitdefender, with a distinct but fairly minor decline through the days of the Response sets and RAP numbers consistently excellent, even the proactive set very well covered. The certification sets caused no problems, and a VB100 award is easily earned, maintaining Bitdefender’s recent run of success and keeping it on 12 passes in the last two years of comparatives. No serious problems were noted, but the failure of the set-up of the man pages was just enough to affect our scoring, meaning only a ‘Stable’ rating is earned.



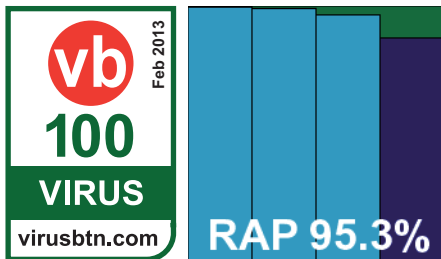
### eScan for Linux File Server

Main version: 5.6.1

Update versions: N/A

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

The developers of *eScan* provided a fairly comprehensive submission: the four main RPM packages, weighing in at 190MB,



were accompanied by a licence file, a dependency list and a PDF user guide. The dependency list proved unnecessary, with all of the requirements already in place on a fairly basic system, and the user guide was only really needed to confirm the order in which the RPMs should be run, and to provide the syntax for changes needed in the *Samba* configuration file. Man pages were provided for the main executable components, but not for the daemons, however configuration was mostly performed via a browser-based

GUI, which proved simple to access and operate, providing ample information and controls for most purposes. Updates were fairly speedy, completing in little over a minute on most runs, although the *ClamAV*-based part regularly reported issues which could only be resolved by updating core components manually; the *Bitdefender* part of the product operated smoothly throughout.

Speeds were not too bad and overheads just a little high, with RAM use around average and CPU use fairly low. Detection scores, as expected, were excellent just about everywhere, showing slight declines into the most recent sets but from very high starting points. No issues were encountered in the core sets, earning *eScan* a VB100 award and putting it on a perfect 12 passes in the last dozen tests. With no stability issues to report, a 'Solid' rating is earned.

### ESET Security for Linux

Main version: 4.0.5

Update versions: Scanner 7818, 7919, 7926, 7943

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

*ESET*'s submission was a nice and compact 60MB single RPM installer, which ran through quickly and simply; final set-up of the product included adjustment of just a single

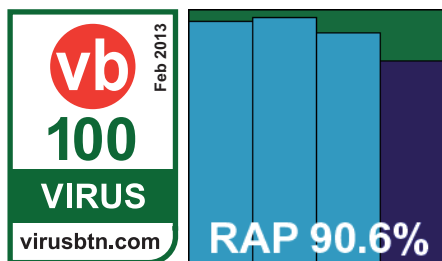
File access lag time (s/GB)	Archive files			Binaries and system files			Linux files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Avast	324.82	337.32	324.82	145.50	143.70	145.50	338.48	338.38	338.48	33.03	32.59	33.03	12.34	13.54	12.34
AVG	135.42	141.88	NA	276.75	269.24	276.75	141.72	143.93	141.72	76.65	72.28	76.65	45.15	46.56	45.15
Bitdefender	170.99	178.04	170.99	151.75	153.00	151.75	330.19	334.41	330.19	67.62	67.57	67.62	47.92	47.17	47.92
eScan	224.44	223.91	224.44	280.13	282.21	280.13	295.00	276.66	295.00	106.19	110.65	106.19	71.94	70.31	71.94
ESET	0.86	1.12	NA	87.37	79.95	87.37	5.05	8.16	5.05	7.11	2.15	7.11	2.83	3.55	2.83
F-Secure	5.45	10.56	723.01	168.49	142.22	179.58	49.77	46.05	2169.52	37.34	33.08	44.06	28.14	28.47	48.45
Kaspersky	6.73	11.05	145.57	135.53	129.21	145.57	45.80	50.10	1186.66	35.54	31.20	37.46	22.70	23.78	27.43
Norman	8.06	911.35	NA	7810.38	7919.09	7810.38	227.53	81.64	227.53	702.72	439.74	702.72	301.94	331.87	301.94
Sophos	0.36	4.23	NA	142.50	131.92	142.50	17.17	21.39	17.17	14.53	9.80	14.53	14.39	14.77	14.39

Please refer to text for full product names.

line in the Samba resource control script and a few tweaks to the product's comprehensive and clearly documented configuration file. Support is also provided for dazuko protection if required. Updates were rapid at around two minutes on average.

Operation is simple and conforms to standard practices, with clear and thorough man pages detailing all components and everything positioned more or less where one would expect to find it. Scanning speeds were decent for the most part, blazing fast over our media sets, and overheads were very low indeed, although we could find no option which would effectively activate archive scanning on access. RAM and CPU use were both around average, and detection was solid, with very consistent and highly respectable scores through the Response sets, a good start in the RAP sets and not too steep a decline into the latter weeks.

The core sets presented no problems as usual, and ESET's epic string of successes continues, with no tests failed or even skipped for many years. No stability issues were encountered, earning the product another 'Solid' rating.

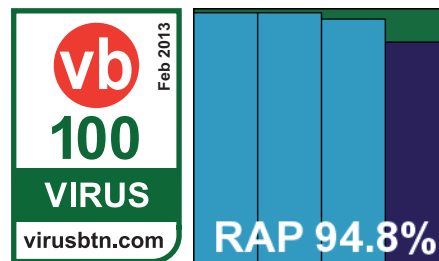


### F-Secure Linux Security

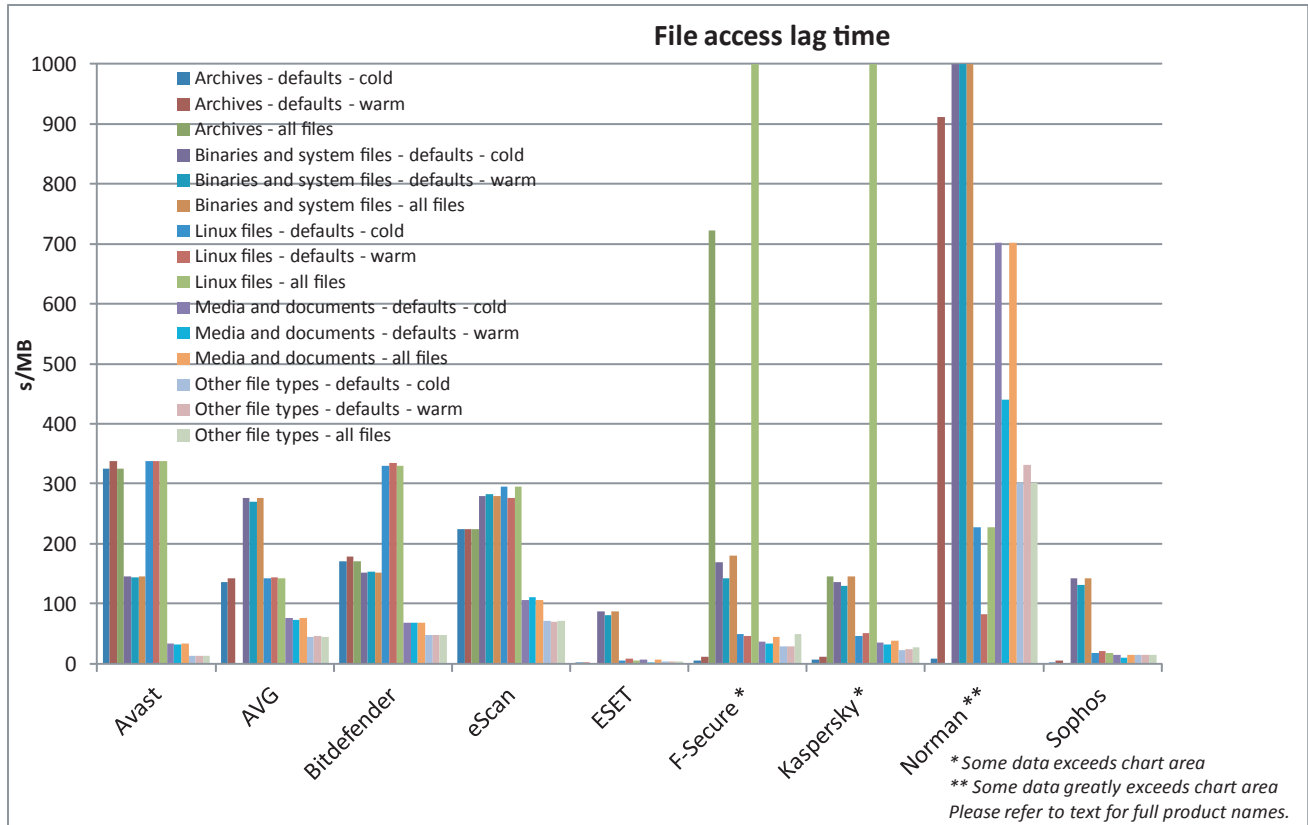
Main version: 9.20.2520  
 Update versions: 2012-12-19\_07, 2013-01-22\_06, 2013-01-24\_06, 2013-01-29\_04

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

The F-Secure product was provided as a slimline 66MB installer, although this lacked updates and had to be installed on the deadline



day to take snapshots of the latest definitions for the RAP tests. The set-up process involved unpacking an archive and running a script contained within it. This seemed to run smoothly, with no major alerts, but on closer scrutiny of the scrolling output, some errors were observed in compiling the dazuko and redirfs modules. Knowing these were not compatible with the kernel in use, we set up a second system with an older kernel. Here, there were no issues and on-access protection operated well, but on the original



machine the product’s browser-based GUI seemed unaware of any installation issues, insisting that protection was fully functional. We also saw some error messages concerning an alternative GNOME desktop interface, which seemed unable to run properly.

With the initial confusion ironed out (the developers informed us that the platform version we were testing on is not officially supported, which makes the problems we noted rather less severe), things moved along nicely. The GUI provided decent levels of information and configuration, and the syntax for the command-line scanner was clear and sensible. Scanning speeds were a little underwhelming, but overheads were mostly decent, although a few sets did slow down considerably when the settings were turned up to the most thorough. Use of memory was very low throughout testing, but CPU use was well up at busy times.

Detection was solid, as we would expect from the *Bitdefender* engine included in the product alongside the company’s own work, with splendid scores everywhere. The core sets were brushed aside comfortably, and a VB100 award is earned. *F-Secure* has a somewhat erratic pattern of submissions of late, and now stands on three passes and one fail from four entries in the last six tests; eight passes and

just that single fail in the last two years. There were a few wobbles observed, including the erroneous assertion that protection was in place when it was not, meaning a stability rating of no more than ‘Fair’.

### Kaspersky Anti-Virus 8.0 for Linux File Servers

Main version: 8.0.2-160

Update versions: N/A

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

Of all the products in this month’s line-up, *Kaspersky*’s inspired the most dread among the test team

vb Feb 2013  
 100 VIRUS  
 virusbtn.com

RAP 89.2%

thanks to difficulties encountered in previous *Linux* tests.

On-demand throughput (MB/s)	Archive files			Binaries and system files			Linux 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	Default (Cold)	Default (Warm)	All files
Avast	8.98	9.12	3.01	14.65	14.92	14.23	1.96	3.09	2.95	24.72	38.55	37.60	34.34	34.81	33.40
AVG	35.90	36.25	4.10	15.18	15.61	15.40	12.18	19.39	1.00	28.54	45.39	43.90	35.25	35.81	35.33
Bitdefender	5.36	5.41	5.36	11.54	11.68	11.54	2.08	3.31	3.25	18.25	28.82	28.47	20.54	20.91	20.54
eScan	5.25	5.29	5.25	14.16	14.38	14.16	2.27	3.58	3.53	24.64	38.58	38.43	34.33	35.07	34.33
ESET	7.73	7.68	7.73	11.80	11.71	11.80	1.86	2.90	2.90	75.60	119.24	117.91	30.52	31.09	30.52
F-Secure	1.42	1.43	1.42	9.04	8.97	9.04	0.36	0.56	0.57	20.05	31.76	31.28	16.47	16.67	16.47
Kaspersky	2.28	2.26	2.28	9.57	9.67	9.57	0.43	0.67	0.67	21.34	33.85	33.28	22.43	21.73	22.43
Norman	4.19	4.23	4.19	11.26	11.19	11.26	2.02	3.17	3.15	34.82	63.28	54.30	36.38	36.95	36.38
Sophos	104.89	131.67	1.68	12.46	12.65	11.42	32.39	51.81	0.21	92.55	148.62	54.88	108.20	109.27	29.74

Please refer to text for full product names.

The initial set-up, from a single 57MB RPM file, was fairly painless and speedy, with a set-up script provided to do the work of compiling and implementing on-access protection, licensing and so on. The on-access component appears to be a custom offering loosely based on the redirfs approach, but there were no problems with getting it set up, and options to protect *Samba* shares explicitly were also provided. Once these first stages were complete, the work of figuring out the configuration and operation process began in earnest, first of all to apply the updates downloaded separately for the RAP tests. This involved lengthy perusal of an epic 178-page user manual (no man pages are provided), and considerable trial and error as the details of adjusting the update process were less than perfectly clear. With no configuration file as such, all changes to settings had to be performed by getting the product to dump the settings of the module in question to a file, tweaking that file and then reading it back in again. In most cases this took some time and a fair amount of brain power. After a while it all became reasonably intuitive, once the basic processes were memorized, but mistakes still occurred disappointingly frequently, meaning testing took far longer than for any of the other products.

In addition, we had some problems getting through the RAP tests, with scans crashing out with errors which hinted at problems in processing log data. This was confirmed by the developers, who provided an alternative syntax to the scan command. This proved more effective, but only after much extra work had been put into trying

to nurse the scanner through the sets. In the end, we saw some fairly slow scanning speeds, especially over our set of archives (which were scanned in-depth by default) and the set of *Linux* files, which included a large number of small files. On-access overheads were excellent though, with low measures across the board, and archive handling still very reasonable when settings were turned right up. RAM use was around average, but CPU use distinctly high.

Detection rates were very good, remaining fairly steady through the Response sets, actually improving in the latter parts, and starting very well in the RAP sets, although dropping quite sharply into the proactive week. The core sets were dealt with properly, and a VB100 award is well deserved, putting *Kaspersky* on six passes in the last six tests; longer term things are a little more shaky, with nine passes and two fails in the last two years. There were a few fairly minor problems this month, which only occurred under heavy stress, earning the product a ‘Stable’ rating.

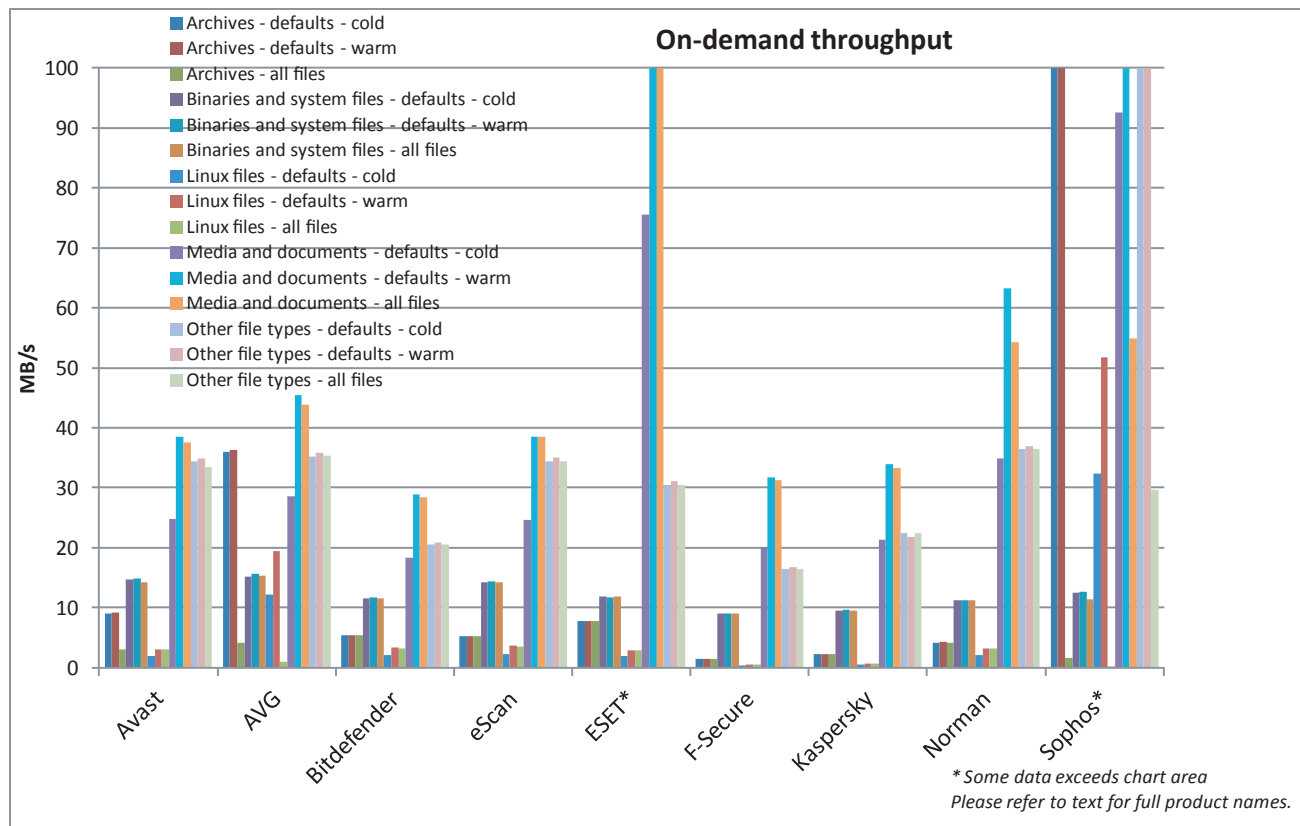
### Norman Endpoint Protection for Linux

Main version: 7.0.20

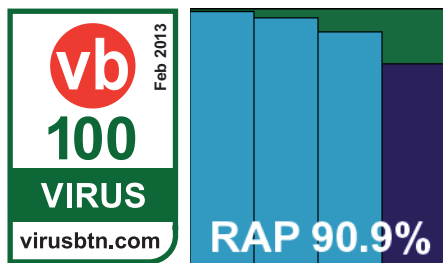
Update versions: 16375682, 17218629, 17285786, 17472528

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





Norman's Linux solution was submitted as a tiny 6.4MB main installer, with 170MB of offline updates for the



RAP sets. This hefty update size was reflected in standard installs, which seemed to complete very rapidly but required considerably more time doing background set-up tasks, much of which seemed to revolve around downloading and implementing updates. Indeed, on at least a couple of installs, the product remained non-functional even after leaving it overnight and giving the entire system a reboot. Most proved reasonably successful after a decent wait though. Configuration was mostly done through another browser GUI, which closely resembled the company's Windows products, making for a pleasant continuity of usage patterns (at least when the GUI could be persuaded to open properly).

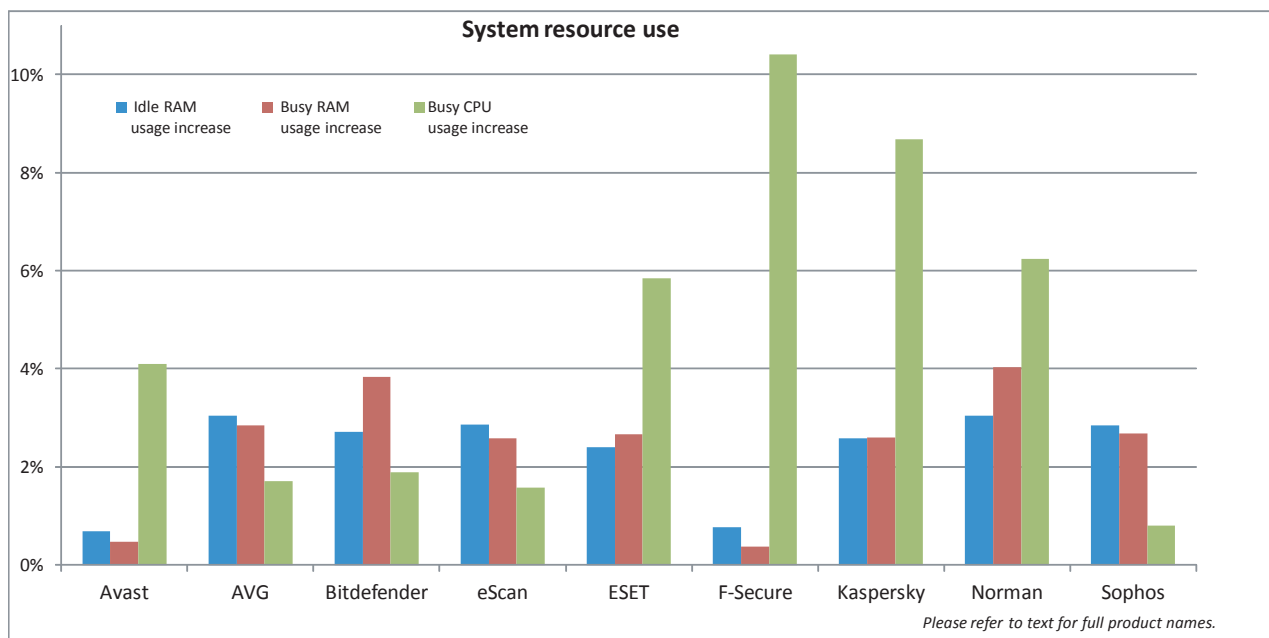
On-access protection is provided using an unusual FUSE-based approach, which worked fine with the

default layout, but we were unable to extend this to cover additional areas. As a result, all our on-access tests had to be repurposed to operate in the /home directory – the only area which seemed to be protected. On-demand scans were a little slow over archives, Windows binaries and Linux files, but reasonable elsewhere. On-access overheads, on the other hand, were fairly heavy for the most part but huge over the set of binary files, with the product's sandbox component clearly adding heavily to the time required to mark files as safe. Some sort of caching of recent results appears to be needed, as much time was spent re-analysing items that had been checked only a few minutes earlier. RAM use was fairly high, and CPU use a little above average too.

Detection was very good though, at least over the older sets, with a fairly sharp drop in the second halves of both the Response and RAP tests. The core sets presented no issues however, and Norman earns a VB100 award. The company now boasts a fairly steady five passes and one fail in the last six tests; ten passes and two fails in the last two years. There were a number of install problems this month, most significantly with trying to apply on-access protection to non-default areas, meaning only a 'Fair' stability rating.

Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase
Avast	0.69%	0.46%	4.09%
AVG	3.05%	2.84%	1.71%
Bitdefender	2.71%	3.84%	1.89%
eScan	2.87%	2.59%	1.57%
ESET	2.40%	2.66%	5.85%
F-Secure	0.77%	0.38%	10.42%
Kaspersky	2.58%	2.59%	8.67%
Norman	3.05%	4.03%	6.25%
Sophos	2.84%	2.68%	0.79%

Please refer to text for full product names.



### Sophos Anti-Virus Protection for Linux

Main version: 4.84.0

Update versions: 2.03.038/3.38.1/4.84, 3.39.0/4.85

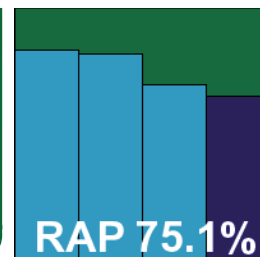
**ItW Std** 100.00% **ItW Std (o/a)** 100.00%

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

**False positives** 0 **Stability** Solid

The last of this month's rather slender field, *Sophos* provided its solution as a 255MB bundle, with separate updates of 6MB. The install runs from a script inside the main archive package, which ran through the set-up,

licensing and initial configuration in a clear and simple manner. On-access protection from the company's



own 'Talpa' service compiled automatically and without problems, and updates were zippy after some initial confusion over an expired licence code. A web admin tool is available but mainly provides information, with most

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Avast	OD	X/√	X/√	X/√	√	√	X/√	X/√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
AVG	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Bitdefender	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
eScan	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	√	√	8	8	√	√	√	8	√	√	√
ESET	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
F-Secure	OD	√	6	6	6	√	6	6	6	6	6	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/6	1/√	1/√	X/√
Kaspersky	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/5	X/√	X/√	√
Norman	OD	√	√	8	3	√	√	√	8	√	√	√
	OA	X	X	1	3	X	X	X	X	X	X	√
Sophos	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X	X	X	X	X	X	X	X	X	√

Key:

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

X - No detection of EICAR test file

X/√ - default settings/all files

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

\* Detection of EICAR test file with randomly chosen file extension









Please refer to text for full product names.

configuration performed by passing commands into the main control binary – a process which is a little fiddly, but reasonably easy to work out thanks to the copious man pages provided. One adjustment, disabling the ‘live protection’ cloud look-up system for the RAP tests, could not be found in the official processes but was simple enough to do by editing an XML config file.

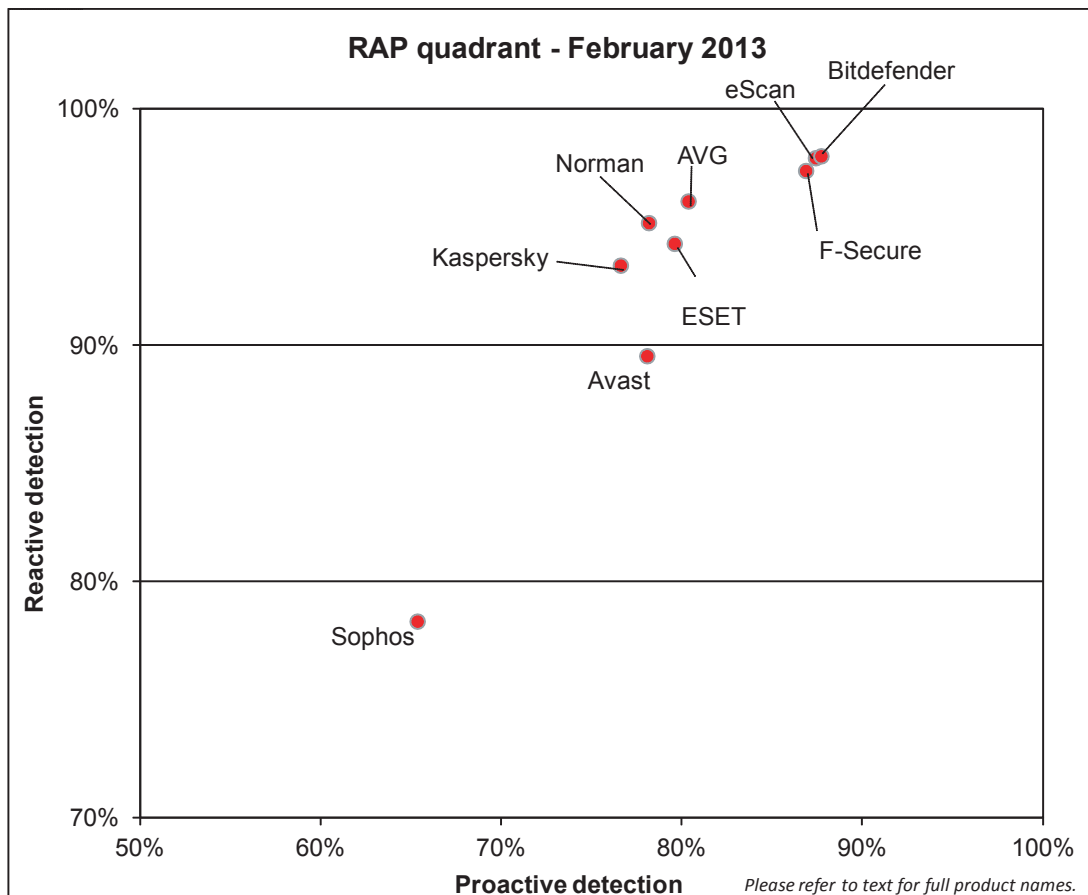
Scanning was very fast indeed, at least with the default settings, slowing down considerably when settings were

extended to cover all file and archive types. Overheads were very light, although it should be noted that the on-access mode is limited to exclude archives. RAM use was average and CPU use very low.

Detection was a little below par in the RAP sets, looking further behind the rest than one might expect thanks to an exceptionally strong field this month, but in the Response sets scores were excellent, demonstrating the effectiveness of the cloud system which should be in place in most

Reactive And Proactive (RAP) tests	VB100	Reactive			Reactive average	Proactive	Overall average
		Week -3	Week -2	Week -1		Week +1	
Avast		83.99%	94.84%	89.85%	89.56%	78.05%	86.68%
AVG		97.40%	98.68%	92.24%	96.11%	80.33%	92.16%
Bitdefender		99.16%	98.57%	96.33%	98.02%	87.69%	95.44%
eScan		99.14%	98.52%	96.15%	97.94%	87.39%	95.30%
ESET		95.29%	96.81%	90.84%	94.32%	79.57%	90.63%
F-Secure		98.21%	98.27%	95.71%	97.40%	86.84%	94.76%
Kaspersky		94.63%	94.99%	90.56%	93.39%	76.58%	89.19%
Norman		98.57%	96.26%	90.75%	95.19%	78.14%	90.93%
Sophos		83.10%	81.93%	69.97%	78.33%	65.33%	75.08%

Please refer to text for full product names.



cases. The WildList and clean sets were handled without incident, and *Sophos* is a worthy winner of another VB100 award, putting it on five passes and one fail in the last six tests; ten passes and two fails in the last two years. Stability was excellent this month, earning a 'Solid' rating.

## CONCLUSIONS

Not quite the clean sweep we had been hoping for, but a pretty near miss, with only one product failing to make the grade (and that was only in one of the three test runs). False positives were absent (perhaps in part thanks to a less extensive than usual update to our clean sets), and the WildList sets were for the most part handled excellently, with just that single momentary lapse from one of the participants.

Otherwise, we saw pretty much what we had expected from the available *Linux* products, some sticking with very simple, standard approaches, others inventing new wheels in bewildering shapes and flavours. Many firms seem content to let their *Linux* solutions slide along with minimal maintenance, while others have clearly invested in bringing them into the 21st century, with all sorts of centralized administration gizmos and multi-function protective layers included.

Stability was generally very impressive, with far fewer problems endured than we would normally expect in a *Windows* test, although whether this is due to the generally higher quality of the participating vendors here, or to the relative simplicity of most of the products, is difficult to judge. Next time we will return to the evergreen *Windows XP*, and expect to see not only a far wider field of products taking part but also a far wider range of issues to vex us.

### Technical details

**Test environment:** All products were tested on identical machines with *AMD Phenom II X2 550* processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Novell SUSE Linux Enterprise Server 11 SP2*, x64 edition. On-access tests were run from a client system running *Microsoft Windows XP SP3* (32-bit), on the same hardware specification. For the full testing methodology see <http://www.virusbtn.com/vb100/about/methodology.xml>.

*Any developers interested in submitting products for VB's comparative reviews, or anyone with any comments or suggestions on the test methodology, should contact [john.hawes@virusbtn.com](mailto:john.hawes@virusbtn.com). The current schedule for the publication of VB comparative reviews can be found at <http://www.virusbtn.com/vb100/about/schedule.xml>.*

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Dr Morton Swimmer

**Test Team Director:** John Hawes

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

**Security Test Engineer:** Simon Bates

**Sales Executive:** Allison Sketchley

**Perl Developer:** Tom Gracey

**Consulting Editors:**

Nick FitzGerald, *AVG, NZ*

Ian Whalley, *Google, USA*

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

## SUBSCRIPTION RATES

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

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

*Corporate rates include a licence for intranet publication.*

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

- Comparative subscription: \$100

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

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

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

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

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

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

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

VIRUS BULLETIN © 2013 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2013/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.