

# virus

## BULLETIN

Covering the global threat landscape

## VB100 COMPARATIVE REVIEW ON UBUNTU SERVER 12.04LTS

### INTRODUCTION

The members of the *VB* test team usually look forward to the annual *Linux* test as something of a break from the much larger comparatives we run on other platforms. With far fewer companies offering *Linux* solutions, the test is always much quieter than those on the *Windows* platforms, and the ease of automating tasks is an additional bonus.

This *Linux* comparative is even smaller than usual: a number of products we might expect to see taking part were notable by their absence, and a handful of other products that were initially entered for the test were found to be incompatible with our testing procedures.

Although the start of the testing period overlapped with the previous comparative, and the end of it threatened to coincide with a rather disruptive lab move, we managed to get through the required tests in fairly decent time, helping us realign our schedule with pre-existing plans.

### PLATFORM AND TEST SETS

*Ubuntu* continues to thrive, combining popularity in the consumer desktop market with strong inroads into server and corporate deployment. According to *Wikipedia*, it runs on more than a quarter of all *Linux*-based web servers. The version used in this test, 12.04 LTS, was released in April 2012 and is the most recent 'Long Term Support' version available.

Installation of the platform is a fairly slick and user-friendly process, in stark contrast to the *Linux* set-up of days gone by, with all of the hardware in our relatively new test machines fully supported out of the box. We opted for a fairly minimal install, with no GUI and only a basic set of software, as this would be the standard set-up in most serious server environments: only necessary items should be installed, for both security and efficiency reasons.

The server systems were prepped with our standard sets of samples and scripts, with this being the last outing of our speed measurement set in its current incarnation – work is already well under way to build a fresh new set. The only change to the speed sets for this test was the addition of a set of *Linux* files, harvested from the main operating directories of a well-used *Linux* server machine.

We would generally advise readers to avoid comparing our speed and performance figures directly between tests, as other variables apply, but it is particularly difficult to compare between our normal *Windows* tests and *Linux* comparatives as there are some fundamental differences in the testing processes employed.

While we try to keep things as similar as possible between tests, including using the same sample sets and automation systems wherever possible, our *Linux* tests operate on two machines: the server for which protection is being tested, and a client from which all on-access tests are performed. This is intended to represent a normal client system connecting to a file server, and either being allowed to access or prevented from accessing various items stored there by the solution under test.

In this case, the client systems ran *Windows 7 Professional SPI*, recycling an image used in a previous comparative with some minor tweaks, and had shares from the test servers mounted as network drives via *Samba*. For the on-access protection tests we simply used the normal scripts we would deploy in a *Windows* comparative, and for speed and performance tests we used slightly tweaked versions of our standard automation. This allowed some simple communication with the server systems, controlling the recording of resource use and so on during the various test phases.

As the set of standard activities used for our main time-delay testing is designed primarily to work on

*Windows*, some sections of it may be less significant here than usual. For example, in the step where samples are downloaded from a local web server, there should be no way for the *Linux* back-end to tell how these files are being written to them, be it a web download or a simple copy from another local location. The rest of the activities, dominated by copy/paste/delete and archiving, should impact the file server in a normal way despite the fact that the script coordinating the actions is running on the *Windows* client.

For the certification tests, we used the latest WildList available on the test deadline of 18 December, which was the November list released that very day. This should be the last time we see separate ‘Standard’ and ‘Extended’ lists, with the two due to be merged before the next comparative.

Our clean sets were updated with a healthy swathe of new items, and pruned to remove older samples where necessary. The final sets used for false positive testing amounted to around 985,000 files, 250GB of data. The remaining test sets – containing malware samples used for the now unified Response and RAP tests – were compiled daily using the latest samples gathered in the appropriate time frame, according to our history of previously encountered samples.

With the prep work all complete, we were ready to get busy looking at the small group of products participating in the comparative.

### AVG Antivirus for Linux

Main version: 13.0.3114

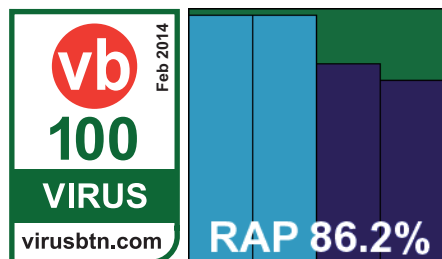
Update versions: 3657/6926, 3681/7005, /7019, /7034

Last 6 tests: 5 passed, 1 failed, 0 no entry

Last 12 tests: 10 passed, 2 failed, 0 no entry

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

AVG’s product is provided in a range of formats including RPM, .deb and simple shell-script installers. We selected the



.deb variant as the most suitable for our systems, and it appeared to install happily. However, initial experiments found many of the main components refusing to operate properly. Some moments of confusion followed, but with a little assistance from the developers, we soon realized that

the product is 32-bit only and so required some additional compatibility libraries to function. With these in place, all seemed fine.

Operation was fairly intuitive, with a handful of main daemons controlled by a set of binaries which are used to pass in settings, and the scanner provided a good range of options in a simple and sensible style.

On-demand scanning speeds were pretty zippy with the standard settings, and slower in most areas with full archive and file type handling enabled. On-access overheads were heavy though, with all our sample sets taking a long time to plod through. Resource use was a little high, and our set of tasks took a fair time to process. There were a few minor issues, mostly down to the confusion caused by absent dependencies, and a Stable rating is earned.

Detection was very good, dropping off fairly noticeably into the later parts of the proactive sets. The WildList and clean sets were handled well, and a VB100 award is earned.

### Bitdefender Security for Samba

Main version: 3.1.2.131213

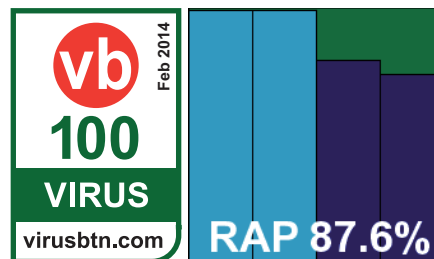
Update versions: 27557

Last 6 tests: 6 passed, 0 failed, 0 no entry

Last 12 tests: 12 passed, 0 failed, 0 no entry

<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

Bitdefender’s *Samba*-focused version is provided as a .deb install package wrapped in a script, which sets most things



up nicely. A few additional manual steps are required to enable the integration with *Samba*, directing share access to the scanner via a VFS object. The configuration system again uses a tool to pass in settings rather than the more standard approach of a human-editable configuration file, but with a little practice the complex syntax proved reasonably usable.

Scanning speeds were not super-fast, with overheads a little heavier than some for simple file reading too. Resource use was low though, especially CPU use, and our set of tasks didn’t take too long to complete. There were no problems with stability, and a Solid rating is earned.

Detection was very good indeed, with superb figures in the reactive sets and pretty good scores in the proactive sets too. The certification sets were dealt with cleanly, and a VB100 award is earned.

### eScan Anti-Virus for Linux

Main version: 7.52159

Update versions: 7.52777, 7.52901

Last 6 tests: 5 passed, 1 failed, 0 no entry

Last 12 tests: 11 passed, 1 failed, 0 no entry

<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

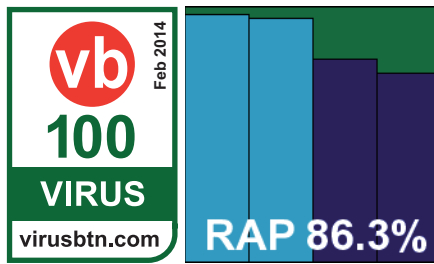
The *Linux* solution from *eScan* came as a handful of *.deb* install packages, plus a fairly lengthy list of dependencies to fulfil before getting started

– which made for a little extra work, but saved us from having to dig around to find out what was required for ourselves. Again, on-access protection is for *Samba* shares only, using the VFS object approach and requiring a little manual tweaking of *Samba* config files to get it enabled.

The product's layout is a little fiddly, with much of the configuration only possible via a web-based graphical interface – meaning that on our GUI-free servers we had to move to another machine to perform changes. For the on-demand scanner at least, full control is available at the local command line, with reasonably clear and sensible syntax.

Scanning speeds were pretty decent, very fast indeed over our sets of *Linux* files, and on-access lag times were very low too. RAM use was a little high at idle, but fine when busy, and CPU use was fairly low too. Our set of tasks was not too heavily impacted, and stability was decent with just a few minor issues accessing our automation tools from the client system (which was blocked initially before access was granted).

Detection was again excellent: reactive sets were not covered quite as well as *Bitdefender*, whose engine is included here alongside *ClamAV* and some additional stuff of *eScan*'s own, but the proactive sets were very well handled, and with no issues in the certification sets, *eScan* also earns a VB100 award.



### ESET File Security for Linux

Main version: 4.0.10

Update versions: 9187, 9293, 9313, 9341

Last 6 tests: 6 passed, 0 failed, 0 no entry

Last 12 tests: 12 passed, 0 failed, 0 no entry

<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 Linux* file server product is also provided as a *.deb* package, and installation was smooth and simple.

For once,

configuration is

provided in the traditional manner with a well-commented config file which can be edited to change settings.

On-access protection is available via a number of approaches, and we opted for the *Samba*-share-only method, requiring just a simple tweak to one of the *Samba* start-up files.

The layout is fairly clear and usable, helped a lot by clear commenting and documentation, and the scanner options are logical and easy to use too.

Scanning was mostly fairly fast, but a little slower than most over our set of *Linux* files, while overheads were pretty low, even with the archive-handling settings turned up. Resource use was low and our set of tasks got through in decent time. There were no stability issues, and the product earns a Solid rating.

Detection was pretty strong, dropping away a little into the proactive sets, but the certification sets presented no problems and a VB100 award is well deserved.

### Quick Heal for Linux

Main version: 15.00

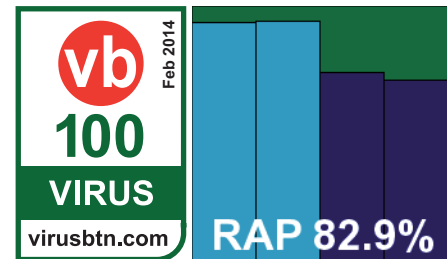
Update versions: N/A

Last 6 tests: 5 passed, 0 failed, 1 no entry

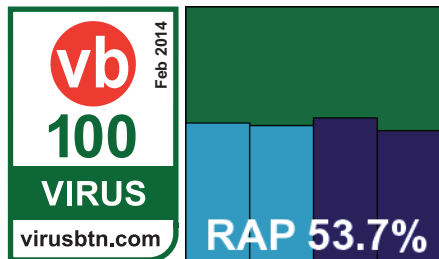
Last 12 tests: 9 passed, 2 failed, 1 no entry

<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

*Quick Heal's* offering was provided as a simple zip file containing an installer shell script, which seemed to set



things up nicely. Again, only *Samba* shares are protected, using the VFS object approach, with a little manual work involved in setting things up.



The configuration is fine-tuned using tools rather than editing simple files, but for the on-demand scanner, options are passed in in the normal manner, with a sensible format.

Scanning speeds were reasonable, but attempting to measure on-access speed, resource use and impact on standard tasks proved rather difficult, with our tools freezing up at the client end as access to *Samba* shares cut out, apparently overwhelmed by the repeated and rapid attempts to access files. We also saw some on-demand jobs crashing out – mainly in the core false positive sets but also in the sets used for speed measures – meaning that we had to repeat a number of the scan attempts. Most of the problems proved to be associated with a couple of reproducible issues, and a Fair stability rating is just about earned.

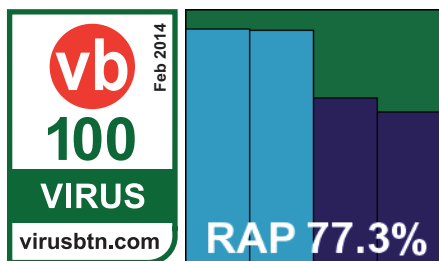
Detection was a little disappointing across the board, but the certification sets were properly handled, with nothing missed in the WildList sets and no false alarms in the clean sets, thus earning *Quick Heal* a VB100 award.

### Sophos Anti-Virus for Linux

Main version: 4.94.0  
 Update versions: 3.48.0/4.96, 4.97.0/3.50.2/4.97  
 Last 6 tests: 6 passed, 0 failed, 0 no entry  
 Last 12 tests: 11 passed, 1 failed, 0 no entry

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

*Sophos's Linux* product promised full on-access protection of the entire system, with previous experience teaching us that the Talpa hooking system used comes



either as a pre-built binary, for major *Linux* versions, or in source form for compilation on-the-fly during the install process. Initial install attempts proved tricky, with the scripted process completing with apparent success but then reporting that the on-access component was unavailable due to unspecified problems. Much research eventually revealed that some of the required build tools were absent from our system. Adding the required tools made everything work nicely, but clearer reporting of the problem would have enabled us to pin it down much more quickly.

The layout again eschews traditional configuration files in favour of a suite of control tools, which can be a little confusing at first but soon becomes fairly usable. Scanning is much more traditional, with a clear and comprehensive set of command-line options.

Scanning speeds were very fast over archives with the default settings, where a list of file extensions is employed, and pretty speedy elsewhere too, even with the settings turned up. Overheads were fairly average, but one set (our set of *Linux* samples) failed to complete properly with archive handling enabled – this is likely to be due to odd file types or deeply nested archives. This was the only issue observed, meaning a Stable rating is merited. RAM use was low, CPU use a little higher than some at busy times, and our set of activities took a surprisingly long time to complete.

Detection was pretty strong in the reactive sets where cloud look-ups are available, dropping quite sharply in the proactive sets where the product does not have the benefit of this technology. The core certification sets were well dealt with, meaning a VB100 award is earned by *Sophos*.

### UNTESTED PRODUCTS

As the test deadline approached we heard from two regular participants in our comparatives, *Avast Software* and *Kaspersky Lab*, who informed us that their respective *Linux* solutions were about to receive a major new version, so it would not be worth testing old and almost obsolete editions in this round of tests.

Products from two additional firms were submitted for testing and quite some time was spent installing and exploring them before we decided to exclude them from the final test. An offering from *Norman* was found only to provide on-access protection in the case of local read actions, and did not protect remote users connected via *Samba*, while a product from *Total Defense* proved to provide on-demand scanning only.

Without proper protection of *Samba* shares, neither product would have qualified for certification, and most of our speed

and performance measures would have been useless, so both were left out of the test.

## CONCLUSIONS

This was a fairly small test, but one which presented its share of difficulties – most of them as usual related to figuring out how to set up and configure products. Many participants provided detailed instructions, others complete manuals, but a few simply handed over an installer and left things up to us, which made for a good test of their products' ease of use. In the end, we managed to figure most things out without too much head-scratching or resorting to contacting developer teams for help.

For the first time in living memory, we have a clean sweep of certification passes, with *all* products reaching the required standard for a VB100 badge. Most also did well in terms of stability, although the problems we saw in one were fairly severe and meant losing a big chunk of the performance data we would have liked to have provided.

*Linux* support seems to be dwindling, or at least being given less priority by the firms that do provide it, but *Linux* systems continue to dominate many areas of the diverse server market, and continue to pick up fans in the consumer world too. So, it's clear that protection is still needed, both to guard servers themselves from nasty *Linux* malware hijacking server credentials and taking over website installations, and to provide an extra layer of defence for clients connecting to file shares and other network resources. Hopefully, this time next year we will see a fuller field of participants.

The next test will be back to the *Windows* platform with *Windows 7*, and we expect many more products to participate. We'll be making a few more incremental adjustments to our tests too, with a few planned expansions of our performance measurement processes alongside the replacement of our speed sets – as well as getting a first look at the new WildList format.

### Technical details

**Test environment:** All tests were run on identical systems with AMD A6-3670K Quad Core 2.7GHz processors, 4GB DUAL DDR3 1600MHz RAM, dual 500GB and 1TB SATA hard drives and gigabit networking, running *Ubuntu Linux 12.04 LTS*, 64-bit Server Edition. Client systems used the same hardware and *Microsoft Windows 7 Professional*, 32-bit edition.

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Dr Morton Swimmer

**Test Team Director:** John Hawes

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

**Security Test Engineer:** Scott James

**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 © 2014 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2014/\$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.



Certification tests	On demand		On access		Clean sets	
	Standard WildList	Extended WildList	Standard WildList	Extended WildList	FP	Warnings
AVG	100%	100%	100%	100%		2
Bitdefender	100%	100%	100%	100%		
eScan	100%	100%	100%	100%		
ESET	100%	100%	100%	100%		
Quick Heal	100%	100%	100%	100%		
Sophos	100%	100%	100%	100%		







(Please refer to text for full product names.)

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
AVG	OD	X/N	X/N	√	√	X/N	X/N	X/N	X/N	X/N	X/N	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Bitdefender	OD	√	√	5	5	√	√	√	4	9	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
eScan	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	√	√	8	8	√	√	√	8	√	√	√
ESET	OD	√	√	√	√	√	√	√	X/N	√	√	√
	OA	X/N	X/N	X/N	X/N	X/N	X/N	X/N	X/5	X/N	X/N	√
Quick Heal	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	2	X	2	2	X	X	X	X	X	X	√
Sophos	OD	X	X/N	X/7	X/7	X/N	X/N	X/N	X/7	X/N	X/N	X/N
	OA	X	X/N	X/7	X/7	X/N	X/N	X/N	X/7	X/N	X/N	√

Key:

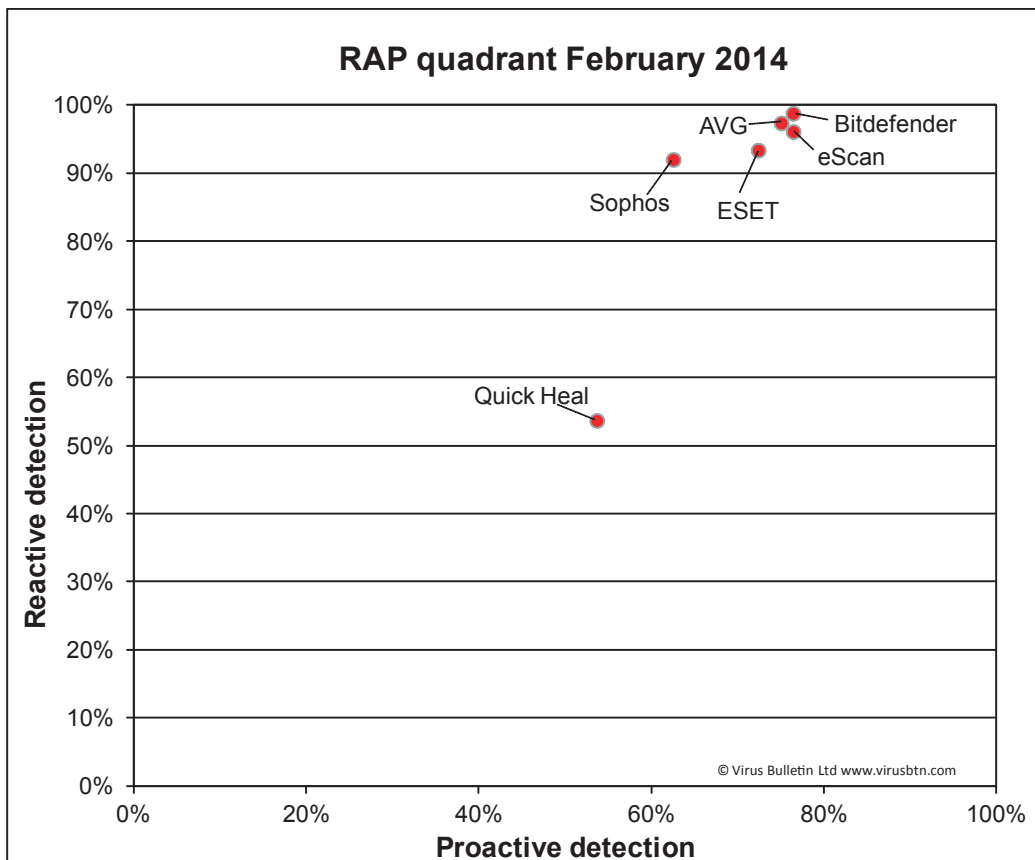
√ - Detection of EICAR test file up to ten levels of nesting  
 X - No detection of EICAR test file  
 X/N - default settings/all files

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.)

Reactive and Proactive (RAP) tests	VB100	Reactive		Proactive		Reactive average	Proactive average	Overall average
		Set -2*	Set -1*	Set +1†	Set +2†			
AVG		97.38%	97.34%	78.29%	71.85%	97.36%	75.07%	86.22%
Bitdefender		98.74%	98.82%	79.15%	73.73%	98.78%	76.44%	87.61%
eScan		96.71%	95.50%	79.17%	73.75%	96.10%	76.46%	86.28%
ESET		93.04%	93.70%	73.83%	70.98%	93.37%	72.41%	82.89%
QuickHeal		54.12%	53.20%	56.20%	51.20%	53.66%	53.70%	53.68%
Sophos		92.02%	91.98%	65.14%	59.98%	92.00%	62.56%	77.28%

\*Set -1 = Samples discovered 1 to 5 days before testing; Set -2 = Samples discovered 6 to 10 days before testing.

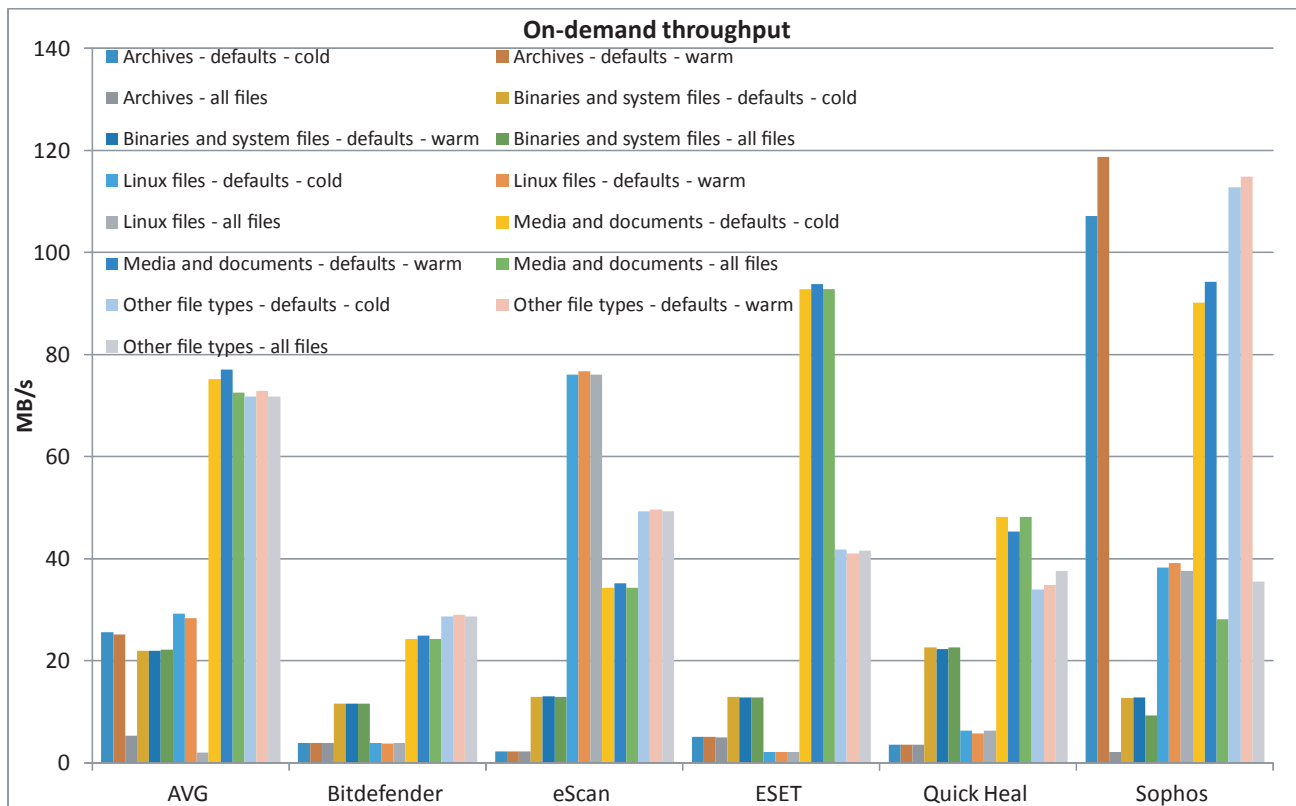
†Set +1 = Samples discovered 1 to 5 days after updates frozen; Set +2 = Samples discovered 6 to 10 days after updates frozen.  
 (Please refer to text for full product names.)



(Please refer to text for full product names.)

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
AVG	25.65	25.17	5.31	22.00	21.95	22.24	29.24	28.32	1.99	75.18	77.01	72.58	71.76	72.86	71.76
Bitdefender	3.90	3.88	3.90	11.57	11.67	11.57	3.85	3.82	3.85	24.29	24.93	24.29	28.70	29.06	28.70
eScan	2.29	2.28	2.29	12.97	13.03	12.97	76.08	76.70	76.08	34.32	35.21	34.32	49.34	49.59	49.34
ESET	5.09	5.07	5.04	12.97	12.88	12.78	2.09	2.11	2.11	92.87	93.79	92.87	41.82	41.01	41.55
Quick Heal	3.54	3.56	3.54	22.63	22.34	22.63	6.36	5.81	6.36	48.21	45.32	48.21	33.95	34.89	37.59
Sophos	107.12	118.76	2.13	12.68	12.86	9.34	38.27	39.14	37.59	90.21	94.25	28.19	112.77	114.82	35.48

(Please refer to text for full product names.)



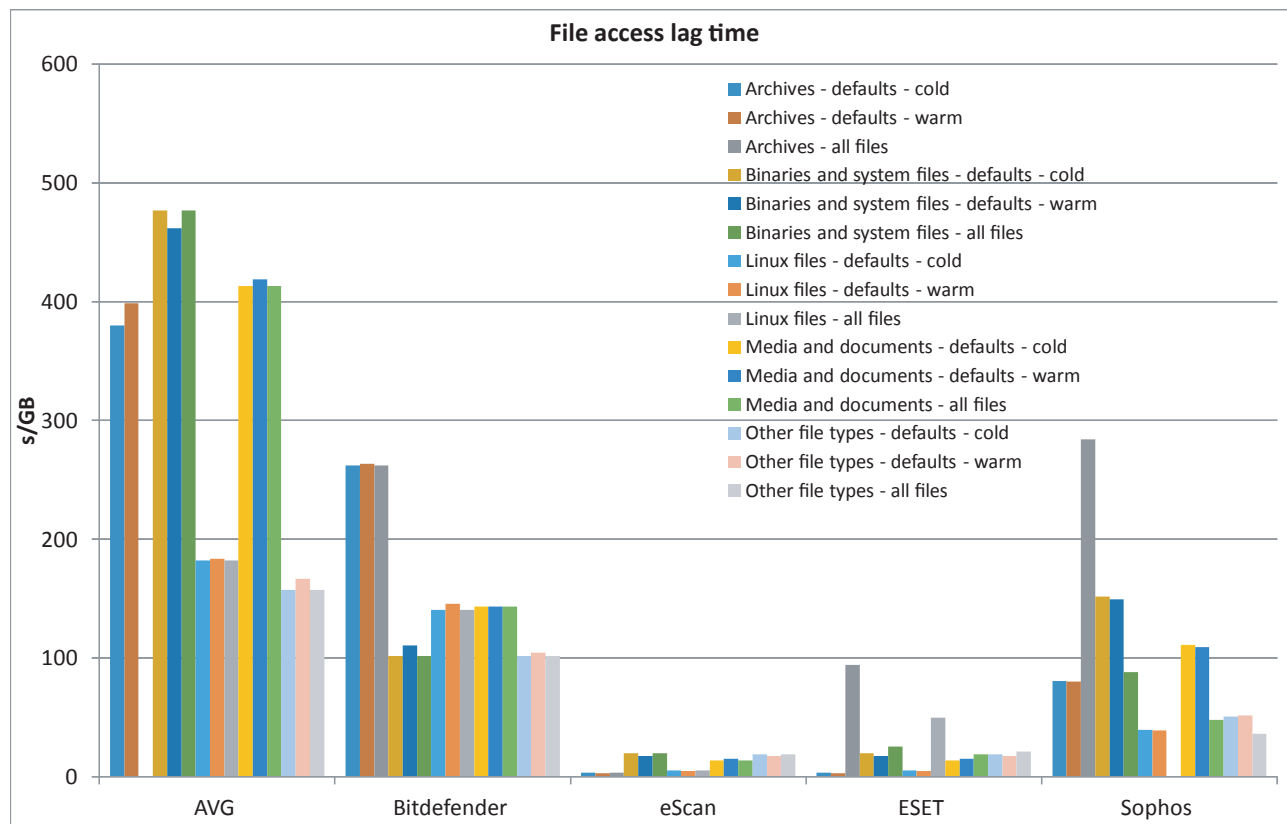
(Please refer to text for full product names.)



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
AVG	379.76	398.63	NA	476.94	461.86	476.94	182.07	183.50	182.07	413.26	418.77	413.26	157.52	166.92	157.52
Bitdefender	262.15	263.71	262.15	101.90	110.62	101.90	140.50	145.56	140.50	143.21	143.21	143.21	101.57	104.73	101.57
eScan	3.53	3.20	3.53	19.84	17.65	19.84	5.35	4.80	5.35	13.98	14.97	13.98	18.98	17.51	18.98
ESET	3.53	3.20	94.07	19.84	17.65	25.23	5.35	4.80	49.77	13.98	14.97	19.10	18.98	17.51	21.17
Quick Heal	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T	N/T
Sophos	80.46	80.07	283.97	151.65	149.60	88.29	39.65	39.13	N/T	110.95	109.01	48.08	50.51	51.79	36.38

N/T - Not tested.

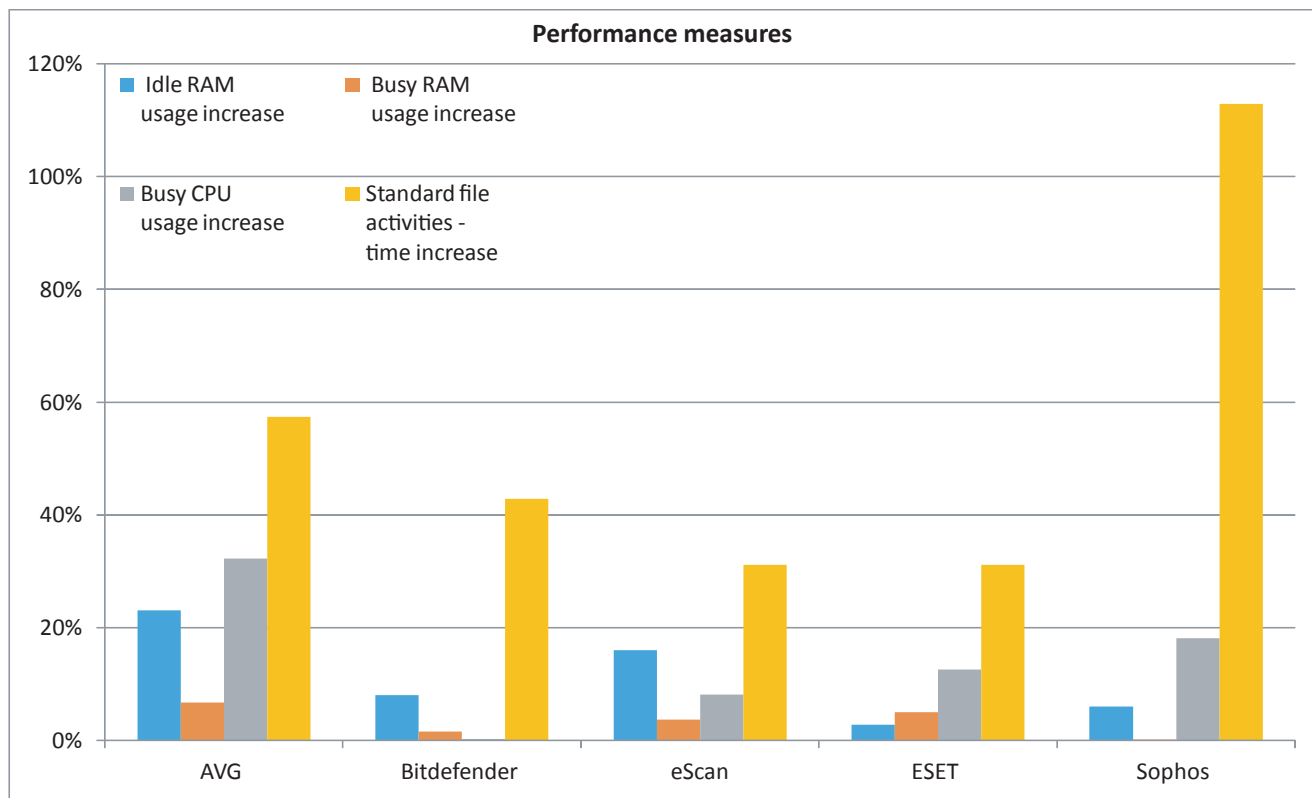
(Please refer to text for full product names.)



(Please refer to text for full product names.)

Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities - time increase
AVG	23.03%	6.67%	32.28%	57.34%
Bitdefender	8.00%	1.59%	0.23%	42.80%
eScan	15.97%	3.62%	8.13%	31.09%
ESET	2.80%	5.00%	12.50%	31.09%
Quick Heal	N/T	N/T	N/T	N/T
Sophos	6.00%	0.08%	18.09%	112.90%

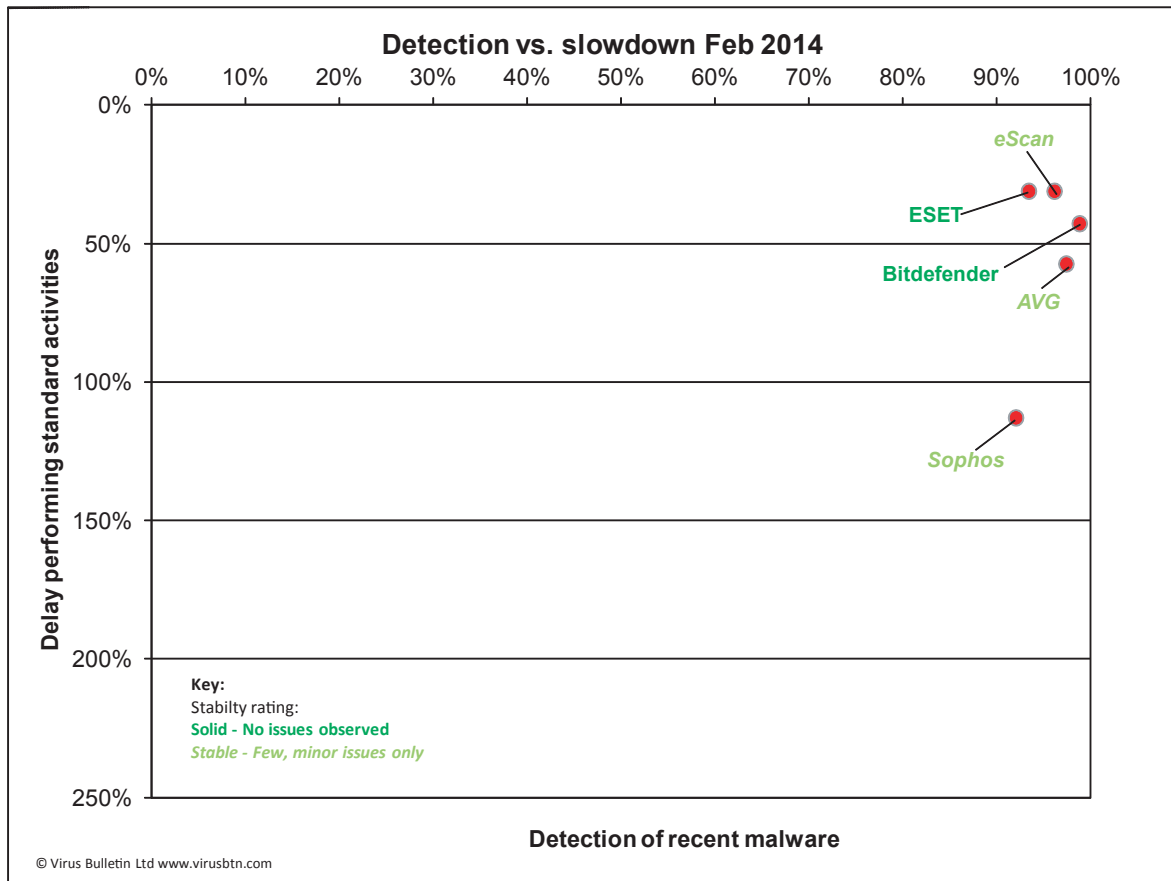
*N/T - Not tested  
(Please refer to text for full product names.)*



*(Please refer to text for full product names.)*

Product information	Install time (m)*	Reboot required	Third-party engine technology	Stability score	Stability rating
AVG	4			2	<i>Stable</i>
Bitdefender	6			0	<i>Solid</i>
eScan	6		Bitdefender	2	<i>Stable</i>
ESET	3			0	<i>Solid</i>
QuickHeal	3			14	<i>Fair</i>
Sophos	5			3	<i>Stable</i>

0 = Solid                      15 - 29.9 = Buggy  
 0.1 - 4.9 = Stable        30+ = Flaky  
 5 - 14.9 = Fair  
 \*Install time including dependencies  
 (Please refer to text for full product names.)



(Please refer to text for full product names.)