

VB100 COMPARATIVE REVIEW ON SUSE LINUX ENTERPRISE SERVER 12

INTRODUCTION

Our annual *Linux* comparative provides a welcome change for the lab team – a different platform, and a very different selection of products. Although the field of competitors for *Linux* tests is invariably smaller than in our *Windows* tests, the process of setting up and operating those products tends to be rather more challenging, with GUIs rare and most of the work done via the command line. This makes finding and figuring out often complex and unintuitive methods of configuring and operating products a much bigger part of the testing process; once the initial deciphering has been dealt with, running the tests tends to be a much faster and simpler process, with these business-oriented products tending to be ruggedly dependable, speedy and simple to automate.

With our schedule of publishing reports still somewhat behind schedule, this report has been kept simple to speed up the process of getting it out to our readers.

PLATFORM AND TEST SETS

The *Linux* variant chosen for this test was *SUSE Linux Enterprise Server 12*, the latest iteration of one of the larger and more serious business-oriented distributions. With the team well-versed in *Linux* installation and operation – using various distributions in our back-end systems and even on the official test machines themselves for forensic and re-imaging purposes – setting up the environment was fairly straightforward, helped by the ever-slicker install systems built into modern professional distributions. Having few enough products for each to reside on a dedicated system for the duration of the test also made things easier.

For testing purposes, each system was set up with a *Samba* share, mounted on a client machine running *Windows 10* to

simulate a user connected to a corporate fileserver; all on-access tests were run from this client.

The selection of products was small but solid, with most of our most regular participants taking part. As is often the case, we had a couple of additional submissions which proved incompatible with our test design or environment, and which were removed from the test after some initial trials.

The test sets were synchronised for the test deadline of 16 December, with tests commencing in early January and complete by early February. The WildList used was v4.024, released on the test deadline day itself. Our other test sets were updated using our standard processes, with the clean sets little changed from previous tests, still weighing in at around 750,000 files, 160GB of data.

RESULTS

Avast for Linux

Main version: 2.1.0

Update versions: 16012000, 16012601, 16020200

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

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

ItW on demand: 100.00% **ItW on access:** 100.00%

False positives: 0 **Stability:** Solid

Avast's Linux solution is fairly simple to install and operate, using RPM install packages, standard init scripts, and pleasingly clear and simple configuration files and command-line syntax. It blasted through our tests with no stability problems or other issues; the only negative noted by the lab team was a lack of on-read protection, all of our on-access tests being done on write instead. This explains

the very low overhead scores in our file access speed measures. Our set of standard activities, which do include a fair amount of

writing to disk, were also very fast though, indicating a light and speedy product all round.

Detection was reasonable, and with a clean run through the certification sets a VB100 award is comfortably earned by Avast.

AVG Anti-Virus for Linux/FreeBSD

Main version: 13.0.3118

Update versions: 4477/11188, 11443, 11490, 11539

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

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

ItW on demand: 100.00% **ItW on access:** 100.00%
False positives: 0 **Stability:** Stable

Also using RPM installers and a set of fairly simple and clear command-line tools for its operations, AVG's Linux solution was

quick and easy to set up and use. Stability was almost perfect, our rating dented only by a single incident of a scan failing to complete. On-demand scanning speeds were very fast indeed, reasonably light on access, with a fairly low impact on our set of activities.

Detection was solid, well up with the rest of the field, and the core sets were handled adroitly, earning AVG a VB100 award.

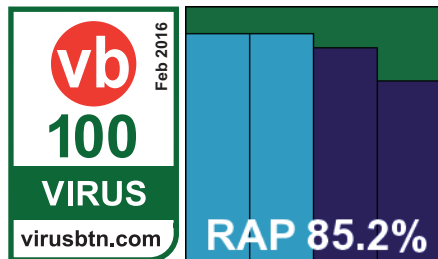
Bitdefender Security for Samba Linux

Main version: 3.10.0.150323(30597)

Update versions: 3.10.0.140729(29018), 7.64245, 7.64304, 7.64371

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

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

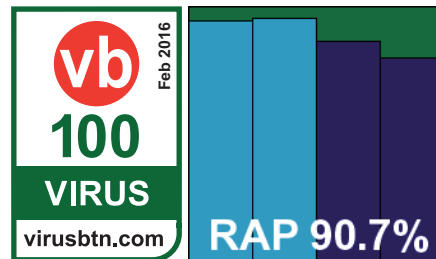


ItW on demand: 100.00% **ItW on access:** 100.00%
False positives: 0 **Stability:** Fair

Bitdefender's installation RPM comes wrapped in a set-up script which helps the user through the basic tasks of getting it up and

running; the command line syntax is a little more complex than necessary but soon becomes intuitive once the basic structure has been figured out, and a web-based console is also provided for those with an aversion to typing. Stability was a little below par, a number of scans crashing out with segmentation faults and updates also failing a few times. Scanning speeds were fairly average but overheads seemed a little heavy, with our set of activities particularly slow to complete.

Detection was excellent though, with good scores everywhere and the product had no problems earning VB100 certification.



eScan Anti-Virus for Linux

Main version: 7.0-3

Update versions: 7.63834, 7.64245, 7.64305, 7.64371

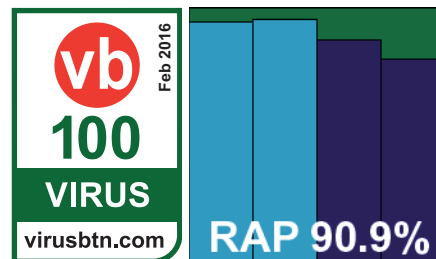
Last 6 tests: 6 passed, 0 failed, 0 no entry

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

ItW on demand: 100.00% **ItW on access:** 100.00%
False positives: 0 **Stability:** Stable

Incorporating the Bitdefender engine, eScan's Linux product requires installation of a number of RPM packages and manual adjustment

of the Samba configuration file to ensure it is protected, but overall the process proved fairly quick and simple. Operation required a dual approach, with most tasks accessible via the command line but some requiring the use of a web interface. Stability was good, with the only issue noted being an oddity with some of our performance testing tools, which repeatedly crashed when trying to run from the



protected share. Following a quick analysis of the problem by the developers, a patch was deployed, which soon fixed this minor issue. Scanning speeds were pretty similar to other participants this month, file access overheads a little on the high side, and our set of tasks ran through in very good time.

Detection rates very closely matched those of *Bitdefender*, as one might expect, and with a good showing across the board a VB100 award is easily earned by *eScan*.

ESET Security

Main version: 4.5.3

Update versions: 12732, 12899, 12929, 12966

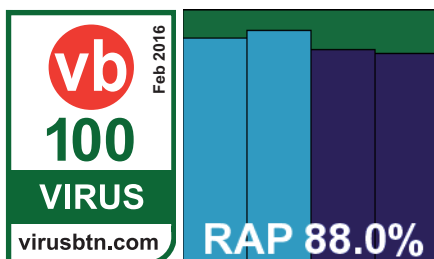
Last 6 tests: 6 passed, 0 failed, 0 no entry

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

ItW on demand: 100.00% **ItW on access:** 100.00%

False positives: 0 **Stability:** Solid

The last entry on this month's rather short list of products is of course *ESET*, yet to miss out on a VB100 award in many, many years. The



vendor's *Linux* edition is provided as a single RPM file, with operation performed properly through traditional configuration files, which proved clear and simple to work with. Stability was impeccable, with no issues observed, and scanning speeds were pretty good too, with a pleasingly light impact on our set of tasks.

Detection was also fairly strong, and with yet another perfect run in the certification sets, *ESET* adds another VB100 award to its huge collection.

UNTESTED PRODUCTS

Additional products were submitted for testing by *iSheriff* and *Norman*; both were found to lack some of the required features and were dropped from the test.

CONCLUSIONS

Linux remains a fairly niche platform on the desktop but holds a strong share of the server market, particularly for web and virtualization purposes. As such, it remains a major target for cybercriminals as well as a simple vector for

spreading malicious infections through an organization, so protection is vital. It's good to see that there is a selection of well-built, dependable products available to admins.

This month's set of products all met the basic requirements of VB100 certification, and went much further in their strong detection rates and useful features. Next time we will be back on *Windows*, with a much wider range of products, and no doubt a correspondingly wide range of levels of quality.

Technical details:

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 *SUSE Linux Enterprise Server 12, SP1*. On-access and performance tests were performed from a client using the same hardware and running *Microsoft Windows 10, 64-bit Professional Edition*, connected to a Samba share on each test server.

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuț Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin






Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

© 2016 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: <https://www.virusbulletin.com/>

Certification tests	On demand	On access	Clean sets		VB100
	Standard WildList	Standard WildList	FP	Warnings	
Avast for Linux	100.00%	100.00%			
AVG Anti-Virus for Linux/FreeBSD	100.00%	100.00%		2	
Bitdefender Security for Samba Linux	100.00%	100.00%			
eScan Anti-Virus for Linux	100.00%	100.00%			
ESET Security	100.00%	100.00%			

Product information	Third-party engine technology	Stability score	Stability rating
Avast for Linux		0	Solid
AVG Anti-Virus for Linux/FreeBSD		1	<i>Stable</i>
Bitdefender Security for Samba Linux		5	<i>Fair</i>
eScan Anti-Virus for Linux	Bitdefender	2	<i>Stable</i>
ESET Security		0	Solid

Stability score: 0 = Solid 0.1 – 4.9 = Stable 5 – 14.9 = Fair 15 – 29.9 = Buggy 30+ = Flaky

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	TBZ2	7z	ZIP	ZIPX	EXT*
Avast for Linux	OD	√	√	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√	√	√
AVG Anti-Virus	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X	X	7	8	X	X	X	X	X	X	X	X/√	√
Bitdefender Security	OD	√	√	8	8	√	√	√	8	8	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√	√	√
eScan Anti-Virus Linux	OD	√	√	8	8	√	√	√	8	8	√	√	√	√
	OA	√	√	8	8	√	√	√	8	8	√	√	√	√
ESET Security	OD	√	√	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/5	X/5	√	√	√	√

Key:

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

X - No detection of EICAR test file

X/√ - default settings/all files

(Please refer to text for full product names.)

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

If just z-exe detection in ext, then X

*Detection of EICAR test file with randomly chosen file extension

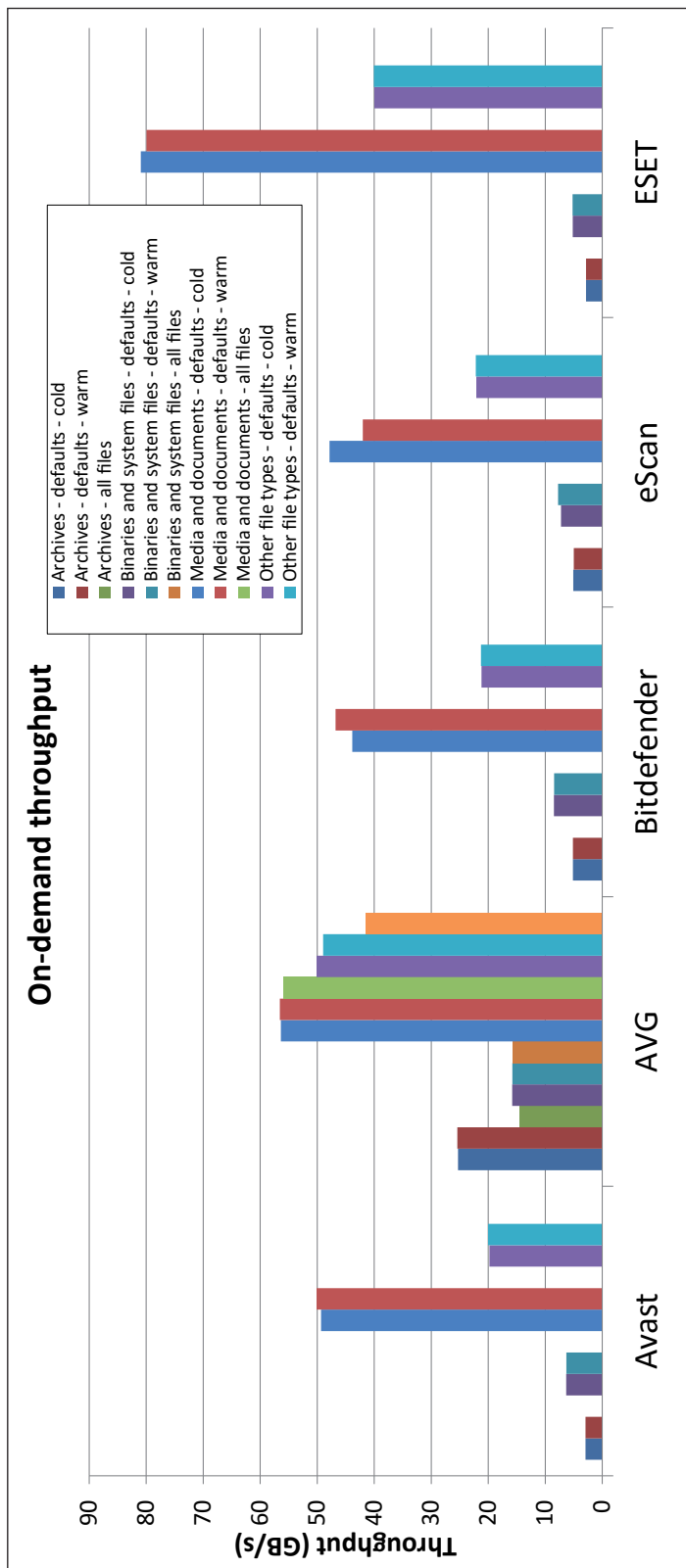
On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Avast for Linux	2.93	2.93	N/A	6.33	6.28	N/A	49.34	50.12	N/A	19.80	20.03	N/A
AVG Anti-Virus	25.29	25.41	14.57	15.79	15.77	15.71	56.38	56.55	55.88	50.12	48.95	41.55
Bitdefender Security	5.14	5.15	N/A	8.46	8.44	N/A	43.85	46.78	N/A	21.19	21.29	N/A
eScan Anti-Virus	5.09	5.01	N/A	7.25	7.74	N/A	47.84	42.01	N/A	22.08	22.18	N/A
ESET Security	2.86	2.86	N/A	5.19	5.21	N/A	80.96	79.94	N/A	39.97	40.05	N/A

(Please refer to text for full product names.)

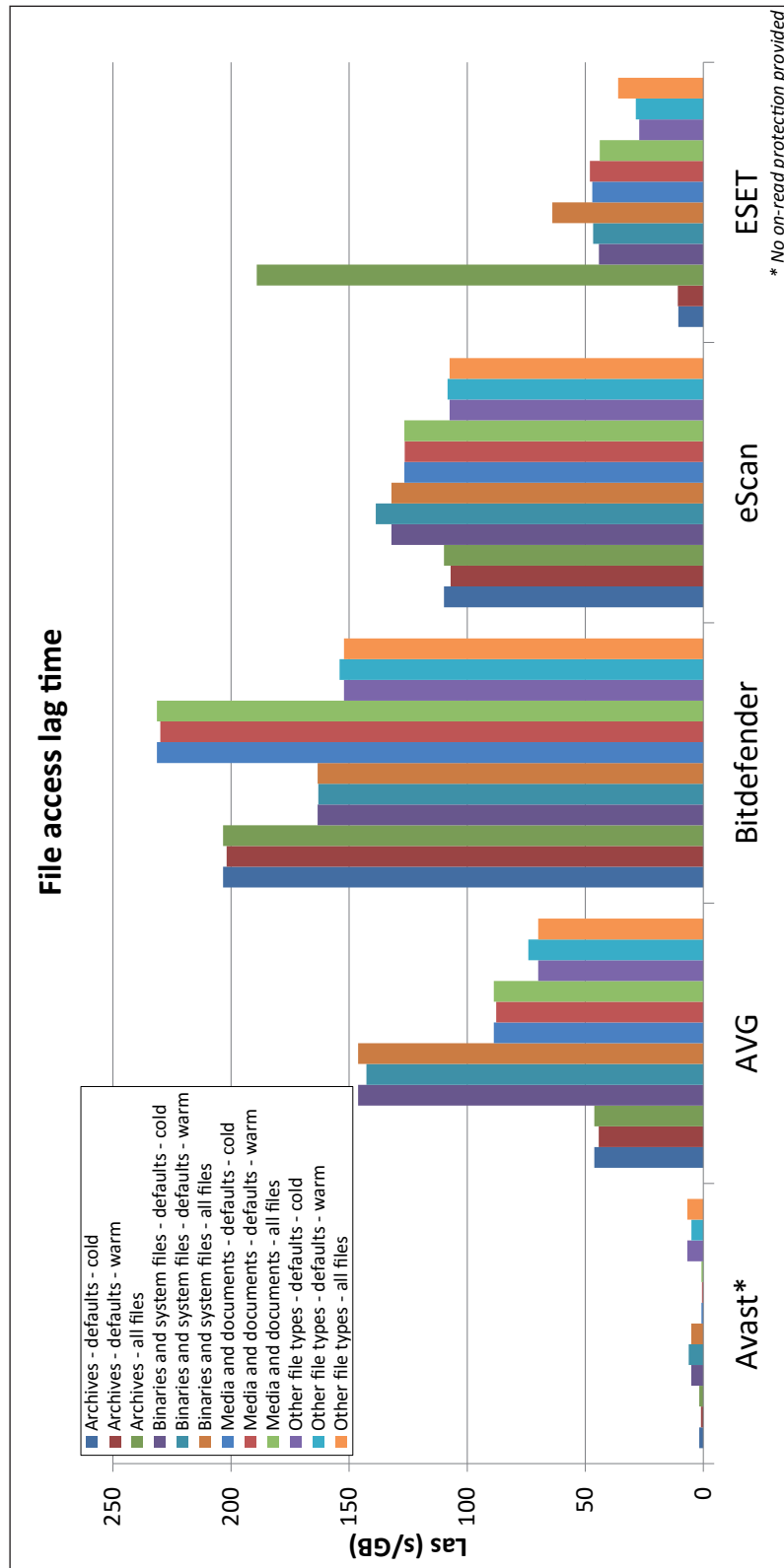
File access lag time (s/GB)	Archive files			Binaries and system files			Media and documents			Other file types			Standard file activities - time increase
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	
Avast for Linux*	1.74	1.07	1.74	5.15	6.26	5.15	0.83	0.61	0.83	6.84	5.05	6.84	1.63%
AVG Anti-Virus	46.17	44.32	46.17	146.21	142.68	146.21	88.72	87.73	88.72	69.91	74.14	69.91	8.95%
Bitdefender Security	203.38	201.82	203.38	163.32	163.01	163.32	231.36	229.91	231.36	152.18	154.04	152.18	247.04%
eScan Anti-Virus	109.85	107.02	109.85	132.04	138.69	132.04	126.60	126.49	126.60	107.43	108.31	107.43	2.73%
ESET Security	10.60	10.87	189.13	44.27	46.65	63.99	47.02	48.07	43.89	27.16	28.64	36.11	5.39%

*No on-read protection provided.

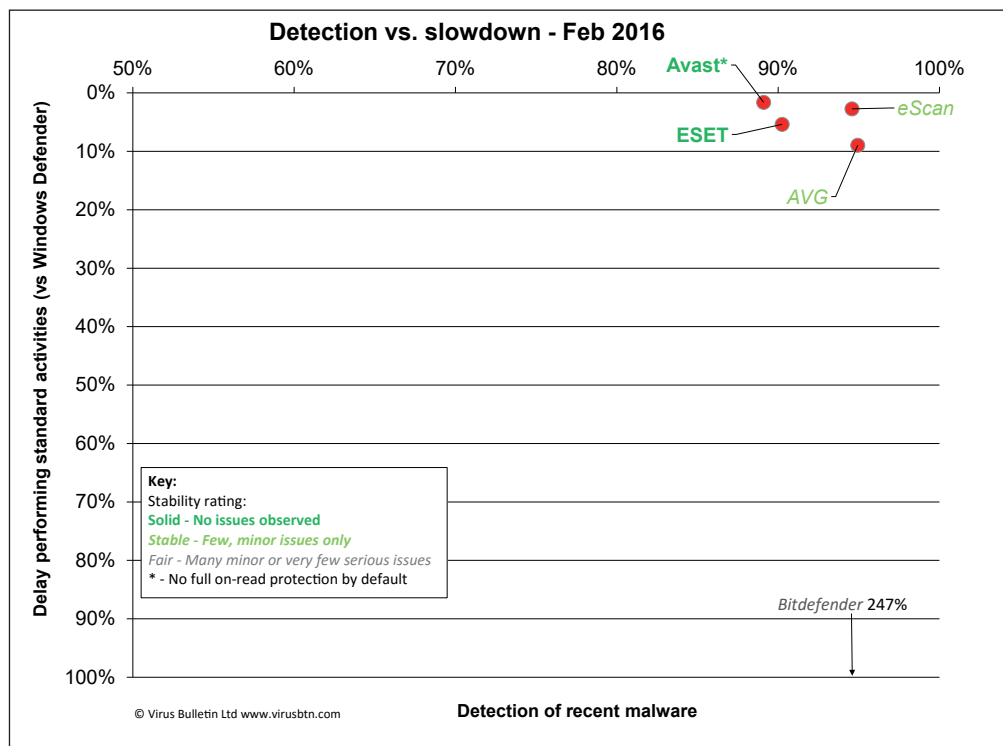
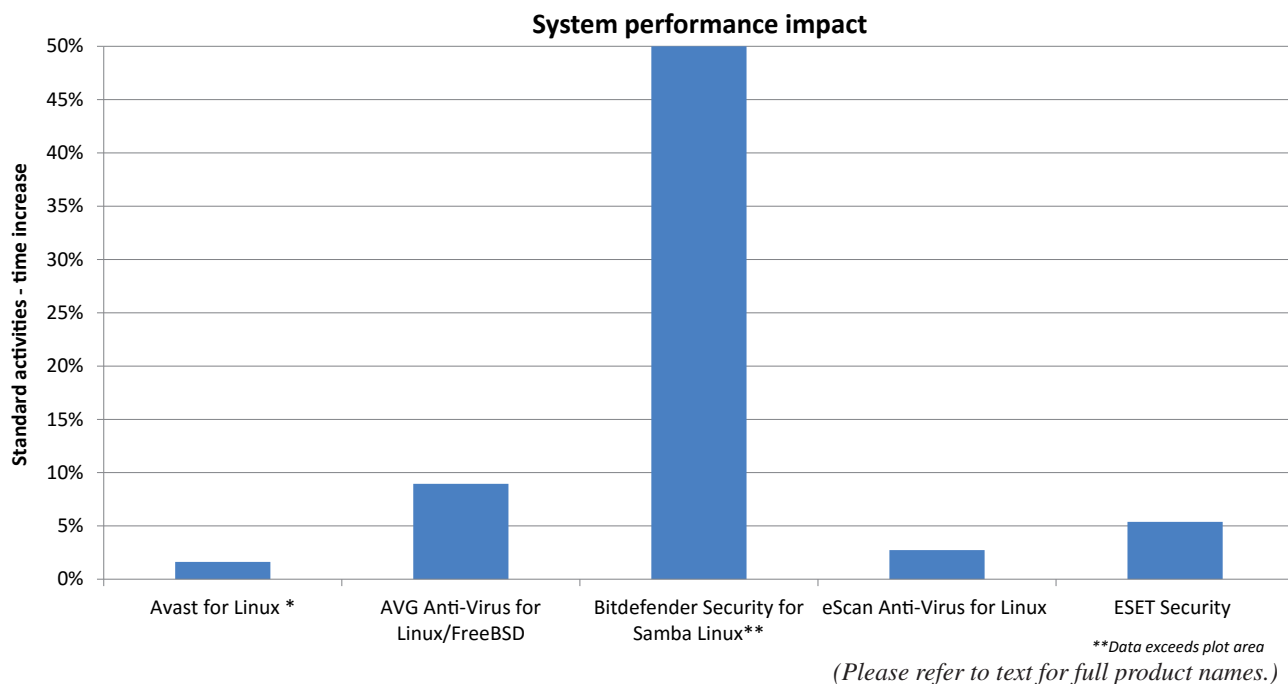
(Please refer to text for full product names.)








(Please refer to text for full product names.)



(Please refer to text for full product names.)



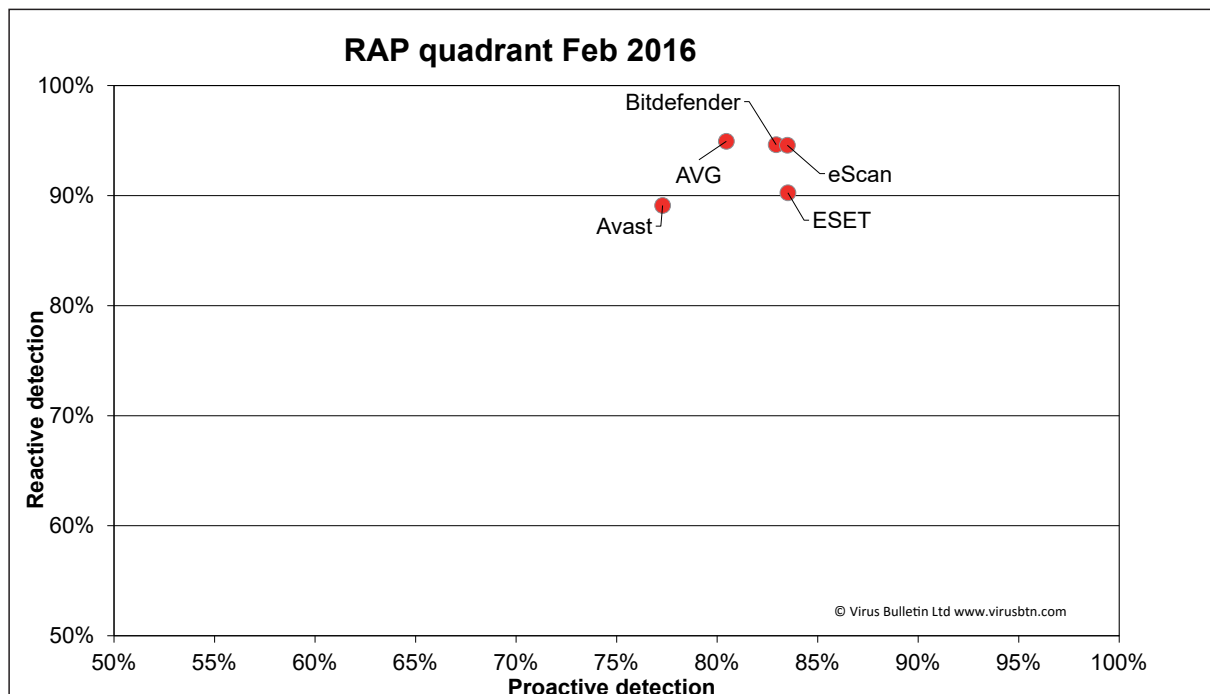
(Please refer to text for full product names.)

Reactive and Proactive (RAP) tests	VB100	Reactive		Proactive		Reactive average	Proactive average	Weighted average [‡]
		Set -2*	Set -1*	Set +1 [†]	Set +2 [†]			
Avast for Linux		89.20%	89.01%	83.62%	70.94%	89.10%	77.28%	85.16%
AVG Anti-Virus for Linux/FreeBSD		94.53%	95.33%	83.50%	77.41%	94.93%	80.46%	90.11%
Bitdefender Security for Samba Linux		94.11%	95.15%	86.00%	79.86%	94.63%	82.93%	90.73%
eScan Anti-Virus for Linux		94.06%	95.08%	87.04%	79.94%	94.57%	83.49%	90.88%
ESET Security		88.68%	91.82%	84.25%	82.79%	90.25%	83.52%	88.00%

*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.

[‡]Weighted average gives equal emphasis to the two reactive weeks and the whole proactive part.



(Please refer to text for full product names.)