



# virus

## BULLETIN

Covering the global threat landscape

## VB100 COMPARATIVE REVIEW ON UBUNTU LINUX SERVER

### INTRODUCTION

This month's report is something of a milestone in the history of the VB100 certification scheme, as it marks the end of a regular cycle of tests going back to the very first comparative in 1998. Since that time our reports have been released in alternate months, each time visiting a different platform to provide the widest possible coverage. However, from the next test things will change considerably, with one of the biggest differences being a focus on the most widely used desktop platforms, *Microsoft's Windows 7* and *Windows 10*, both of which will be covered in each bi-monthly report.

This does not mean we are about to abandon *Linux* users, or indeed server admins who, for whatever reason, are required to use *Windows*; we plan to include comparative reviews on these and other platforms separately from the regular VB100 schedule – details should emerge once the new testing patterns have had a chance to settle in. For now, here are the results of the last *Linux* test, for a short while at least, and the last test in the current format.

### PLATFORM AND TEST SETS

The platform we tested on this month was *Ubuntu Linux 16.04.2 LTS Server* edition, a widely deployed distribution which challenges the major commercial *Linux* variants, and the likes of *CentOS*, for space in the world's data centres. Set-up of the platform is fairly straightforward for anyone with basic *Linux* experience, thanks to ever-slicker graphical tools, and we found that once it was installed, little further effort was required to get our test machines fully operational. When trouble strikes, the *Ubuntu* world is blessed with a huge and active community ready to advise, assist or criticize, but the test team had minimal need of assistance.

We assembled our usual sample sets, starting with the set compiled from the latest WildList available on the test deadline (21 December), which was WildList v4.035, released that very day. Our standard set of clean files saw its final outing before being replaced with an all-new set in the next test, but was still subjected to the usual process of filtering and updating, removing older and less widely used items in favour of newer versions and new packages. Finally, our RAP sample sets were compiled from all samples first seen by *VB* in the appropriate time frame, with a maximum age of ten days at the time of testing. As usual for our *Linux* tests, the sample sets used for our speed measures were supplemented with an additional set of *Linux* files, acquired by gathering together all files from the main binary storage folders of several *Linux* variants. Some of our automation tools were adjusted slightly to fit in with the environment, and as usual all on-access testing was performed from a *Windows* client system attached to a fileshare on the protected server – this month's selection was a *Windows 10* client.

With all the preparations made, the usual rather select group of *Linux* products was put to the test.

### Avast For Linux

Main version: 2.1.2

Update versions: 16122102, 17010500, 17011001, 17011702

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

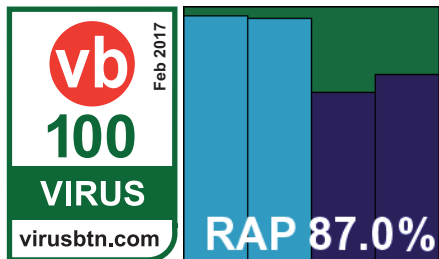
Last 12 tests: 12 passed, 0 failed, 0 no entry

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

**False positives:** 0 **Stability:** Stable

*Avast's Linux* product comes in a .deb format for easy integration into the *Ubuntu* package-management subsystem, and proved pretty simple to set up and operate.

On-access protection is provided on-write using the fanotify system, updating is set up as part of the install process using a cron job, and the main scanner utility has clear and straightforward syntax. Operation was for the most part smooth and steady, although we did note that a single scan job crashed out; repeating the same job got things done with no further problems.



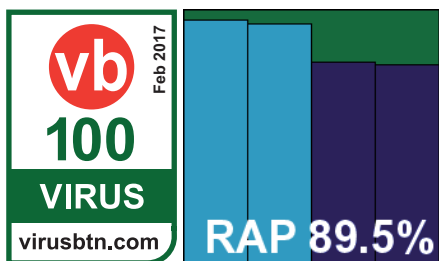
Scanning speeds were decent, file access overheads very light thanks to an absence of on-read checking, and our set of activities was minimally impacted. Detection rates were strong, dropping off somewhat into the offline/proactive parts of the sets, and the certification sets proved no problem with complete coverage of the WildList and no false alarms, earning *Avast* yet another VB100 award.

### Bitdefender Endpoint Security

Main version: 6.2.16.48  
 Update versions: 7.68648, 7.68944, 7.69065, 7.69186  
 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

*Bitdefender's Linux* offering is provided as a classic tar.gz file containing an installation script which did all the work. Once set up, operation takes a little getting used to: there are no standard config files to edit, instead a graphical interface is included for those who like such things, and for others a set of simple tools is used to pass commands into the product. Adding a path to cover on-access protection proved straightforward, and operating the scanner was also not too difficult after a little initial exploration and familiarization.



Stability was impeccable, with no problems noted, and speeds were good too, with only a light slowdown on

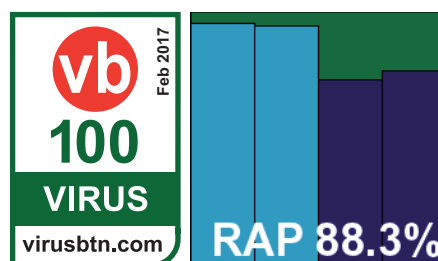
file access and very little impact on our set of activities. Detection was as strong as ever, with good scores across the board, and another good showing in the certification sets earns *Bitdefender* another VB100 award.

### eScan Anti-Virus For Linux

Main version: 7.0-5  
 Update versions: 7.68634, 7.68945, 7.69065, 7.69186  
 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

The *Linux* solution from *eScan* came as a trio of .deb files, with a set of dependencies with which the package manager dealt



easily. Configuration proved best accomplished using a web-based management portal, which seemed clear and usable, and on-access protection is achieved by adding some lines to the *Samba* config file, pointing it to a VFS object. A separate desktop GUI is provided for on-demand scanning, but a command-line option is also available and this was used for the bulk of testing.

Stability was almost perfect, marred only very slightly by part of the interface repeatedly insisting the product required activation, despite all activation steps having been performed. Scanning speeds were decent, although overheads were a little higher than the rest of the field with a noticeable slowdown of our set of activities. Detection, aided as usual by the *Bitdefender* engine, was of course very strong, and with no issues in the core certification sets *eScan* comfortably picks up another VB100 award.

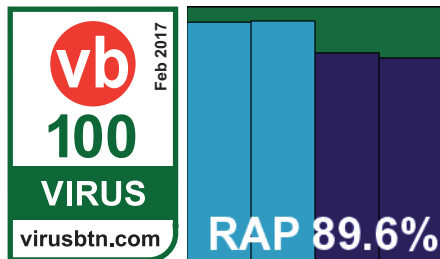
### ESET File Security for Linux/FreeBSD

Main version: 4.5.6  
 Update versions: 1069/14643, 14719, 14750, 14788  
 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

*ESET's* contribution to the *Linux* world is pleasingly simple,

provided as a single .deb package with a single dependency requiring filling. Once installed, it proved similarly easy



to operate with all configuration stored in a single config file. Scanner syntax was clear and comprehensive, and everything ran very smoothly with no issues noted.

Speeds were good, overheads very light, and detection was very strong indeed. Yet another perfect run through the certification sets earns ESET another VB100 award, adding to the vendor’s mammoth collection.

### CONCLUSIONS

As is usually the case for our Linux comparatives, this month’s field of participants was rather small, and with all of them coming into the test with a perfect record of passes over the last few years, it wasn’t much of a surprise that all of them managed to meet the certification requirements. Stability was also pretty good with only a few minor problems observed, and for the most part design and usability was pleasing too. There are doubtless some less than ideal options available to Linux admins, but none of those were submitted for testing this month.

Going forward, as mentioned earlier, a raft of changes are fast approaching. Starting in April 2017 we will be moving to a new VB100 testing process and a new approach to platform selection, with the leading versions of Windows for desktops featuring in our regular bi-monthly tests and other platforms appearing as special events. The tests themselves will be adjusted somewhat to allow our team to focus on developing new, more realistic testing methods, and reports will likewise be simpler with less text and more focus on

the data. Performance testing will be removed from the main test line and spun out into a standalone set of tests to be run periodically.

Although a new team will be implementing these plans, the designs have evolved from the existing set-up and have been in development for some time. The core of the VB100 will remain little changed, with certification still dependent on full coverage of the WildList and no FPs in our official set of clean files.

This is not only the last report in this format, but also the last by this reporter. After 64 comparatives and almost 2,000 products (of which over 1,500 achieved certification), it will fall to others to run the VB100 comparatives and award scheme into the future, which will doubtless be done with both style and rigour. As always, we welcome your feedback and questions, comments and complaints – please email vbstest@virusbulletin.com.

#### 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 Ubuntu Linux Server 16.04.2 LTS. Client systems used the same hardware and ran Microsoft Windows 10 x64 Pro.

**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  
 © 2017 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England  
 Tel: +44 (0)1235 555139 Email: editor@virusbulletin.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%			
Bitdefender Endpoint Security	100.00%	100.00%			
eScan Anti-Virus For Linux	100.00%	100.00%			
ESET File Security for Linux/FreeBSD	100.00%	100.00%			

Product information	Third-party engine technology †	Stability score	Stability rating
Avast For Linux		1	<i>Stable</i>
Bitdefender Endpoint Security		0	<b>Solid</b>
eScan Anti-Virus For Linux	Bitdefender	1	<i>Stable</i>
ESET File Security for Linux/FreeBSD		0	<b>Solid</b>

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

† Only records presence of third-party scanning engines, most products will include additional in-house technologies

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

Key:

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

X - No detection of EICAR test file





X/√ - default settings/all files

(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

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		96.3%	95.1%	66.2%	73.2%	95.7%	69.7%	87.0%
Bitdefender Endpoint Security		95.5%	94.3%	79.1%	78.4%	94.9%	78.7%	89.5%
eScan Anti-Virus For Linux		95.4%	94.2%	73.3%	76.9%	94.8%	75.1%	88.3%
ESET File Security for Linux/FreeBSD		93.7%	94.3%	81.7%	79.7%	94.0%	80.7%	89.6%

\*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.

On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Linux files			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	7.00	7.01	7.00	4.62	5.00	4.62	15.71	17.02	15.71	5.55	5.59	5.55	10.83	12.23	10.83
Bitdefender	14.57	14.76	14.57	5.09	5.98	5.09	14.52	16.01	14.52	5.82	5.87	5.82	15.76	16.63	15.76
eScan	10.23	9.91	10.23	5.08	5.19	5.08	12.49	11.55	12.49	3.14	3.51	3.14	7.13	8.45	7.13
ESET	5.26	5.26	5.26	5.17	5.20	5.17	17.65	17.95	17.65	7.49	7.42	7.49	16.65	16.75	16.65

(Please refer to text for full product names.)

File access lag time (s/GB)	Archive files			Binaries and system files			Media and documents			Linux files			Other file types			Standard 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	Default (cold)	Default (warm)	All files	
Avast	15.10	5.83	15.10	34.96	28.19	34.96	10.48	2.15	10.48	6.91	1.43	6.91	4.09	2.90	4.09	1.03%
Bitdefender	17.00	16.33	N/A	151.24	149.15	151.24	54.99	51.72	54.99	80.29	81.83	80.29	61.00	58.07	61.00	3.71%
eScan	79.16	79.46	79.16	254.46	217.91	254.46	105.35	96.06	105.35	172.69	166.88	172.69	96.05	87.84	96.05	41.39%
ESET	3.39	3.64	84.38	49.53	47.79	48.49	23.57	22.16	22.08	78.07	28.10	27.51	14.72	13.92	13.28	3.94%

N/A = Not applicable. (Please refer to text for full product names.)

