FEBRUARY 2015

virus BULLETIN

Covering the global threat landscape

VB100 COMPARATIVE REVIEW ON RED HAT ENTERPRISE

INTRODUCTION

Once again our annual *Linux* test rolls around, giving the lab team the chance to take a break from *Windows* and dabble with something a little different. This time we return to *Red Hat*, with another rather reduced field of participants and the usual opportunities for simple automation making for a pleasantly low-interaction test, giving us time to work on several long-planned projects to improve and expand our data collection.

In general, stability is better with simpler command-line products, but hopes of a trouble-free ride don't usually last long in the *VB* test lab and we stood prepared to dive in and try to diagnose any arcane issues we might encounter. As usual with *Linux* products, we expected to see a range of interesting approaches, likely to test to the utmost our ability to uncover odd install and configuration methods.

PLATFORM AND TEST SETS

Red Hat's commercial *Enterprise Linux* product line has been around for over a decade now, gradually evolving over time. As is generally the case with *Linux* versions designed for long-term stability, it lacks a few of the bells, whistles and shiny surfaces adopted by more aggressively cutting-edge distros. The install process is nevertheless reasonably user-friendly and clear, with some handy basic admin tools for those not keen on digging into the nitty-gritty of configuration files.

All of our test systems were deployed with a matching image featuring basic tools including file server components. A client running *Windows 7* was attached to each, using a *Samba* share as a network drive. All test sets were deployed to this share, and our standard performance tests tweaked slightly to allow them to be run from the *Windows* machines, with the *Linux* servers recording some performance data in parallel.

The test sets included the most recent WildList available on the 17 December test deadline – the v4.012 list, which was released on the same day. The clean sets used for false positive testing were updated with a selection of common business packages, and a selection of *Linux* samples harvested from a range of different *Linux* versions were also thrown into the mix. The sample sets used for our RAP tests were compiled daily using the latest new samples seen by our lab on each of the appropriate dates.

With all we needed in place, it was time to get our hands dirty and try out the products.

Avast for Linux

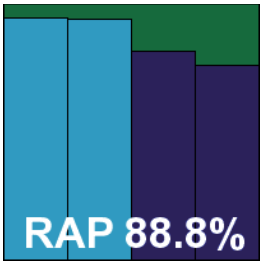
Main version: 1.1.8

Update versions: 14121700/15010600/15011200/15011900

Last 6 tests: 4 passed, 2 failed, 0 no entry

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

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



Avast's *Linux* server solution was provided as a pair of RPM installers, which proved simple and effective. The main daemons are controlled using start-up scripts and options, and the command-line scanner is also clean and clear with simple settings.

The main point of interest was the on-access protection, which covers shared folders on-write only, with no on-read

ISSN 1749-7027

blocking. Enabling it should be as simple as pointing it at the shares you want to be covered and starting up the daemon, but we found that this wasn't always the case, with some of our efforts failing to get it to run properly and leaving the file share inaccessible from our client. We soon got the hang of things though, and got it alerting on attempts to write dangerous items to the share.

Scanning speeds were a little on the slow side, with our standard file access speed measures rendered unusable by the lack of on-read scanning, but our set of activities showed only a small slowdown. Other than the odd start-up issues, stability was decent.

Detection was strong across the board, with good scores in the reactive sets and just a slight trailing off into the proactive areas. The WildList was covered without any problems, and there were no false alarms in the clean sets, earning *Avast* a VB100 award.

AVG for Linux

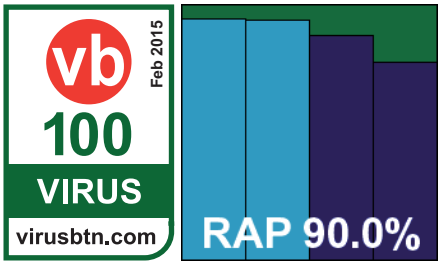
Main version: 13.0.3114

Update versions: 4235/8758, 8881, 8914, 8959

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

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

ItW on demand	100.00%	**ItW on access**	100.00%
False positives	0	**Stability**	Solid



AVG's *Linux* solution came as a single RPM file providing a selection of daemons and tools, with decent usage instructions and fairly clear syntax. Configuration is mostly achieved by passing commands into the various modules rather than the more old-school method of editing files, but is reasonably simple once you've got the hang of it.

Enabling the on-access protection was as simple as passing in a path and enabling a daemon, and it seemed to work nicely from the off.

Scanning speeds were pretty fast over all file types, and although file access lag times were noticeable, they were not too heavy. Our set of tasks showed fairly minimal slowdown, and there were no problems with stability.

Detection was very good indeed, with good scores even into the later parts of the RAP sets, and the certification sets were handled well, earning *AVG* a VB100 award.

Bitdefender Security

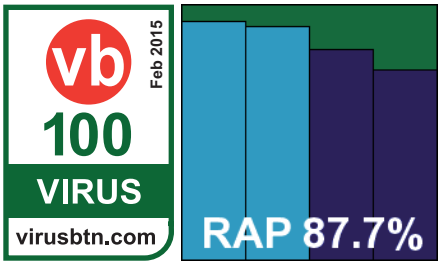
Main version: 3.10.0.141211

Update versions: 29818

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



Bitdefender's solution was provided as a scripted RPM installer which just required executing and following some basic questions and answers.

The on-access component uses a VFS object to cover specific *Samba* shares. This must be dropped into place, then the *Samba* services restarted, with just a few small tweaks required to get it active and optimized. Operations are performed by passing in commands to a suite of tools. Configuration is adjusted in this manner too, although traditionalists will find it more user-friendly simply to dump the configuration out to a file, make alterations there and read it back in again – a process which is also fairly straightforward.

Scanning speeds were pretty decent, but accessing files on the share did seem rather slow, and once again our set of activities took a very long time to complete (something we are continuing to investigate). Stability was mostly OK, but we did note a number of scans crashing out with segmentation fault errors, and also observed some lack of complete activity recording in the logs.

Detection was strong, with a gradual decline through the RAP sets. The clean and WildList sets presented no problems, earning *Bitdefender* another VB100 award.

eScan for Linux File Server

Main version: 5.8-0.el.7

Update versions: 7.58346, 7.58704, 7.58809, 7.58931

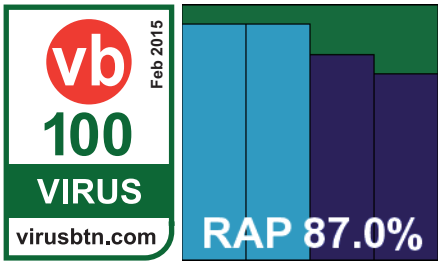
Last 6 tests: 6 passed, 0 failed, 0 no entry

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

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

The *Linux* file server solution from *eScan* arrived as four separate RPM packages which needed to be put in place

in order. The developers provided an extensive list of dependencies, but most of these were already in place on a fairly basic *Red Hat* install.



Some edits to the *Samba* configuration file were required to activate the on-access protection, which was again provided via a *Samba* VFS object. Configuration is mainly performed from a web interface, which is fairly clear and simple to navigate, but hard-core admins may find it annoying not to be able to monitor or make all required adjustments from the command line. A lengthy and detailed manual is provided along with the install bundle, as a PDF document.

Scanning speeds were fairly average, but we ran into a number of snags in the on-access speed and performance tests. Some parts of the performance measure seemed to upset the product somewhere, causing the *Samba* share to lock up and become inaccessible, repeatedly interrupting the flow of our automated measuring system. Despite our best efforts, no data could be gathered in this area. Given the loss of connectivity to the file share, this was treated as a fairly serious problem, and the product's stability is rated only 'Fair'.

Detection elsewhere seemed good though, with high scores in the reactive sets and not too much of a decline into the proactive parts of the sets, and the WildList and clean sets were handled well too. A VB100 award is earned by *eScan*.

ESET File Security for Linux/BSD/Solaris

Main version: 4.0.10

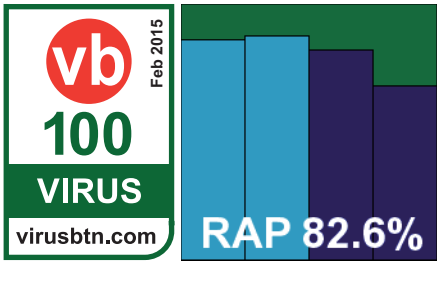
Update versions: 1.055/10890, 10972, 10999, 11037

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 multi-NIX solution is another single RPM installer with just a single dependency we found we had to fulfil for compatibility. A suite of control tools is provided, which all seemed well documented with clear and sensible syntax, and configuration is performed using the tried-and-trusted approach of editing configuration files.



For on-access protection, a few small additions are required to some of the *Samba* control files and the solution's own configuration, which must be followed by a restart of the services to get things up and running nice and easily.

Scanning was a little slow over archives and binaries but very rapid elsewhere, and the impact of the protection on the time taken to access files on the protected share was minimal, only noticeable over archives with the settings turned up to the max. Our set of activities also ran through very rapidly, barely showing any slowdown over the baseline measures, and stability was rock-solid throughout.

Detection was decent, with reasonable scores in the response sets and not too steep a decline into the proactive sets. There were no issues once again in the core certification sets, and *ESET* comfortably extends its epic run of VB100 success with yet another award.

Kaspersky Anti-Virus for Linux File Server

Main version: 8.0.2.256

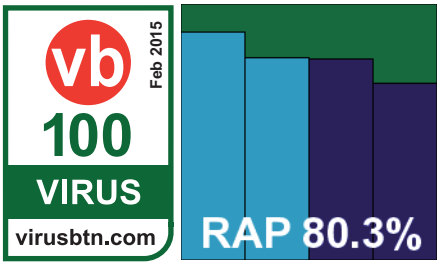
Update versions: N/A

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

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

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

Last up this month is *Kaspersky*'s offering, which has caused quite some head-scratching in the past, but after several runs in the last few years is almost starting to make sense to the lab team. Another single RPM sets everything up nicely, with a set-up process asking the most important questions. Control is provided from a series of tools, the main one helpfully being labelled 'kav4fs-control', and increasingly complex strings of commands are passed in via these in lieu of the more usual configuration file method. Once again, those clinging onto the old ways can output the whole lot into a file, edit it, and read it back in – an approach we found increasingly useful.



The on-access component can operate in a range of ways, but in our case a simple *Samba* VFS approach seemed the most suitable and required minimal effort to set up, the product inserting the appropriate lines into the *Samba* config file and getting everything working nicely in next to no time.

Scanning wasn't the fastest, and accessing files showed a noticeable, if not excessive slowdown, with a similarly clear impact on the speed of our set of standard activities. Stability was mostly good, but one scan did seem to freeze up and had to be restarted.

Detection was OK, with a very gentle decline through the response sets, and the core sets were dealt with easily, earning *Kaspersky* another VB100 award and rounding off a successful month for all participants.

CONCLUSIONS

As usual in our *Linux* comparatives, the field of players was small and all participants have both long and distinguished histories in our tests and international reputations – helping to keep horrors and headaches to a minimum. But as is also the norm, there was plenty of room for confusion and bewilderment as the various diverse approaches had to be figured out and implemented.

Results were strong, with a clean sweep of passes once again, and for the most part excellent detection rates and stability. Our performance measures were rather curtailed this month as we focused on development of the latest version of our more in-depth *Windows* measuring system – a new and more regular version of which we hope to unveil in the next few months. Stability was mostly very good indeed, with little to complain about in most cases, perhaps mainly thanks to the absence of graphical interfaces; these seem to be the area most likely to introduce wobbles.

Next up is another jumbo *Windows* comparative (*Windows 8.1*). At the time of writing, testing is already complete with just the processing of results and compilation of the report to come, so we hope to have that available shortly. As usual, we welcome any comments, complaints, suggestions or criticisms, and hope to continue to improve and expand our testing offerings.

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 *Red Hat Enterprise Linux 7, Standard x64 Edition*. On-access and performance tests were performed from a client using the same hardware and running *Microsoft Windows 7 64-bit Professional Edition*, with SP1, connected to a *Samba* share on each test server.

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. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/

Certification tests	WildList detection on demand	WildList detection on access	Clean sets		VB100
			FP	Warnings	
Avast	100.00%	100.00%			VIRUS 100
AVG	100.00%	100.00%			VIRUS 100
Bitdefender	100.00%	100.00%			VIRUS 100
eScan	100.00%	100.00%			VIRUS 100
ESET	100.00%	100.00%			VIRUS 100
Kaspersky	100.00%	100.00%		3	VIRUS 100

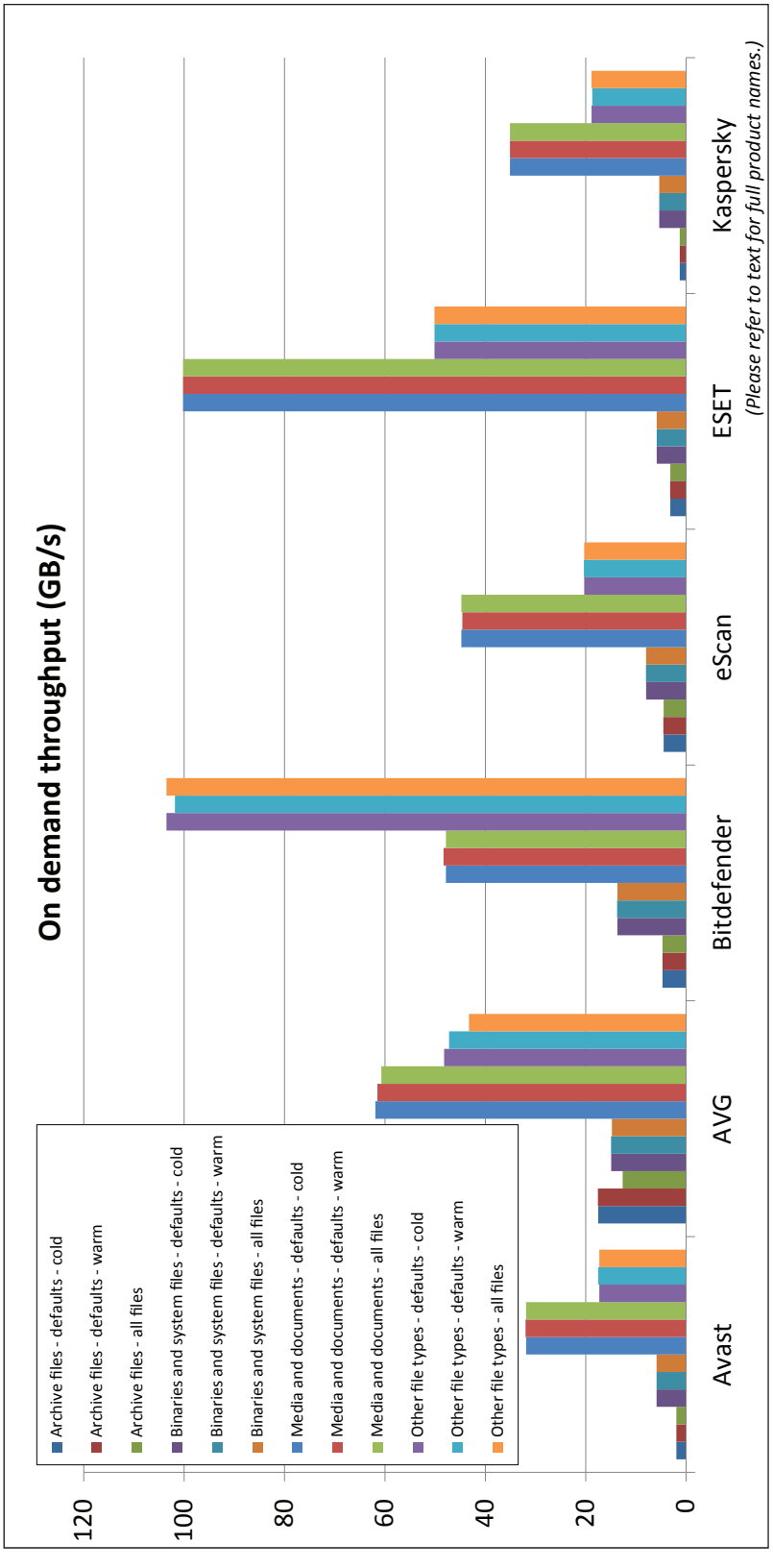
(Please refer to text for full product names.)

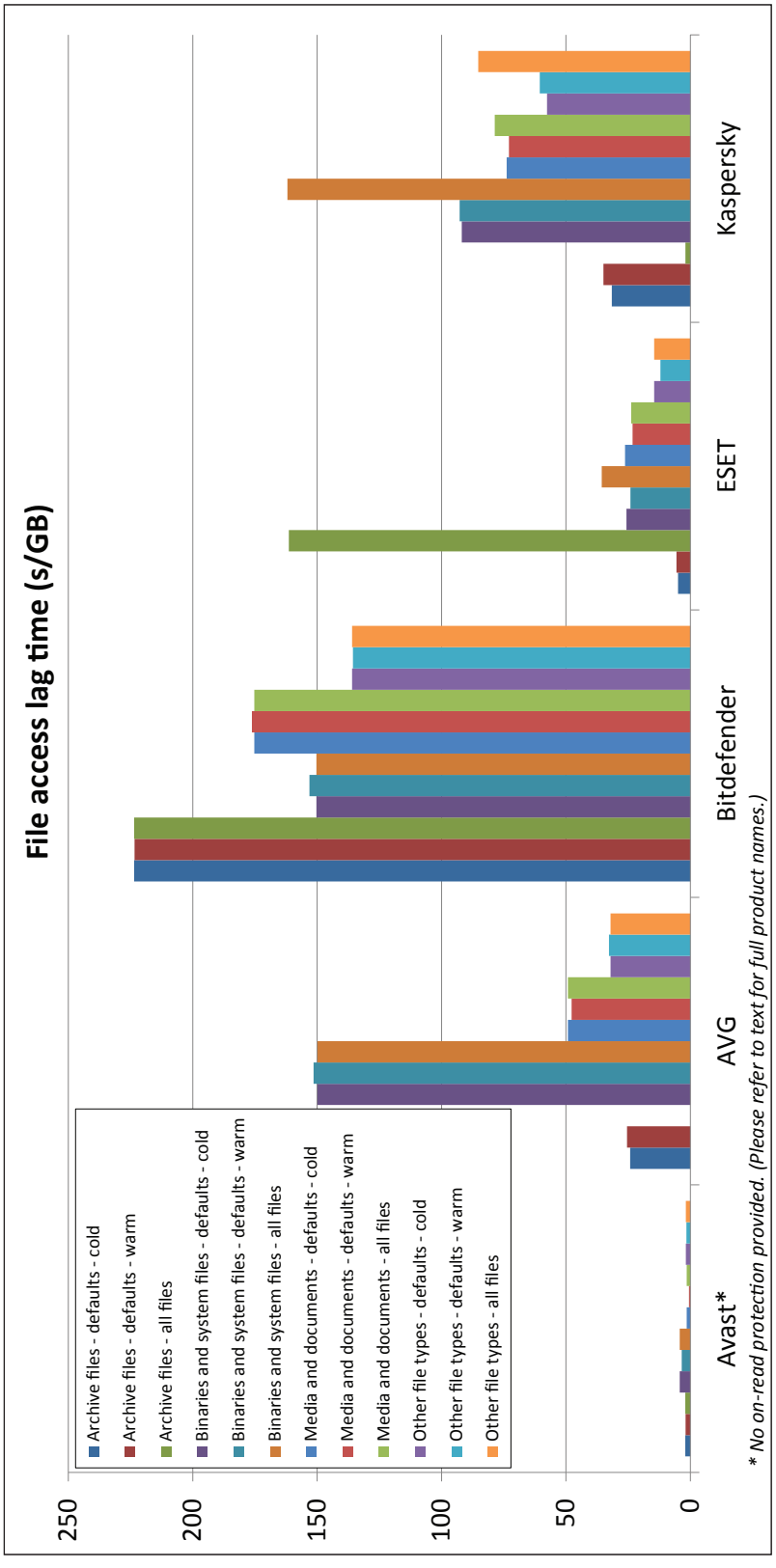
On-demand throughput (MB/s)	Archive files			Binaries and system files			Media and documents			Other file types		
	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Avast	1.95	1.95	1.95	5.88	5.88	5.88	31.89	32.00	31.89	17.30	17.53	17.30
AVG	17.51	17.57	12.65	14.93	14.95	14.79	61.91	61.51	60.72	48.21	47.24	43.25
Bitdefender	4.69	4.69	4.69	13.70	13.75	13.70	47.84	48.33	47.84	103.52	101.85	103.52
eScan	4.47	4.52	4.47	7.96	8.00	7.96	44.79	44.58	44.79	20.31	20.35	20.31
ESET	3.16	3.17	3.16	5.85	5.85	5.85	100.24	100.24	100.24	50.12	50.12	50.12
Kaspersky	1.26	1.26	1.26	5.35	5.35	5.35	35.08	35.08	35.08	18.85	18.70	18.85

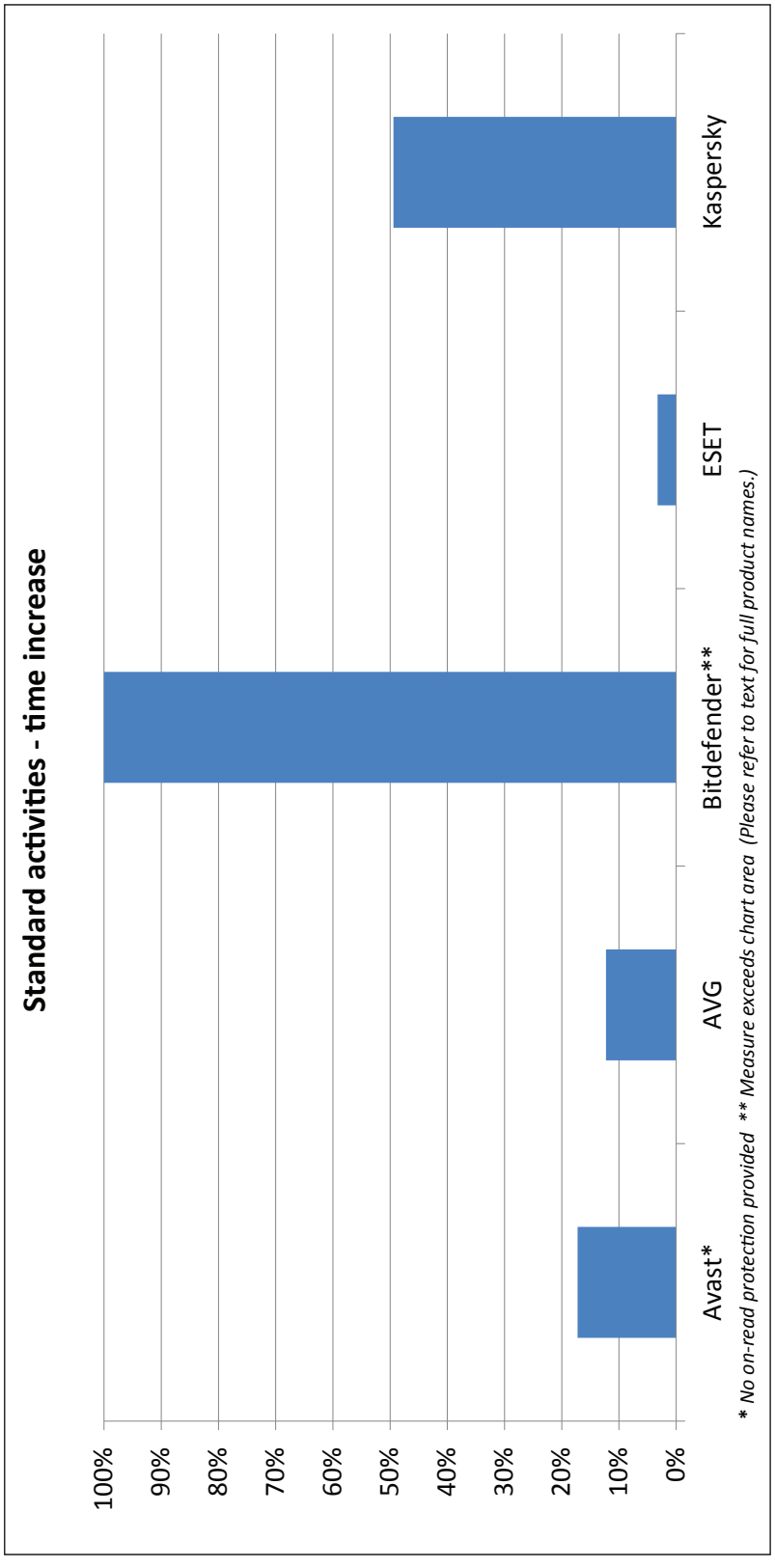
(Please refer to text for full product names.)

File access lag time (s/GB)	Standard activities - time increase	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*	17.25%	2.06	1.94	2.06	4.26	3.49	4.26	1.49	0.59	1.49	1.80	1.62	1.80
AVG	12.27%	24.22	25.46	NA	149.90	151.45	149.90	49.24	47.75	49.24	32.09	32.72	32.09
Bitdefender	558.10%	223.58	223.38	223.58	150.30	153.08	150.30	175.26	176.25	175.26	136.00	135.62	136.00
eScan	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
ESET	3.25%	5.00	5.57	161.38	25.69	24.12	35.62	26.28	23.22	23.82	14.56	12.06	14.56
Kaspersky	49.43%	31.58	34.94	1.98	91.86	92.74	161.93	73.85	72.95	78.62	57.62	60.54	85.29

No on-read protection provided. N/T - not tested. (Please refer to text for full product names.)


On demand throughput (GB/s)
120
100
80
60
40
20
0
Archive files - defaults - cold
Archive files - defaults - warm
Archive files - all files
Binaries and system files - defaults - cold
Binaries and system files - defaults - warm
Binaries and system files - all files
Media and documents - defaults - cold
Media and documents - defaults - warm
Media and documents - all files
Other file types - defaults - cold
Other file types - defaults - warm
Other file types - all files
Avast
AVG
Bitdefender
eScan
ESET
Kaspersky
(Please refer to text for full product names.)


File access lag time (s/GB)
250
200
150
100
50
0
Archive files - defaults - cold
Archive files - defaults - warm
Archive files - all files
Binaries and system files - defaults - cold
Binaries and system files - defaults - warm
Binaries and system files - all files
Media and documents - defaults - cold
Media and documents - defaults - warm
Media and documents - all files
Other file types - defaults - cold
Other file types - defaults - warm
Other file types - all files
Avast*
AVG
Bitdefender
ESET
Kaspersky
* No on-read protection provided. (Please refer to text for full product names.)

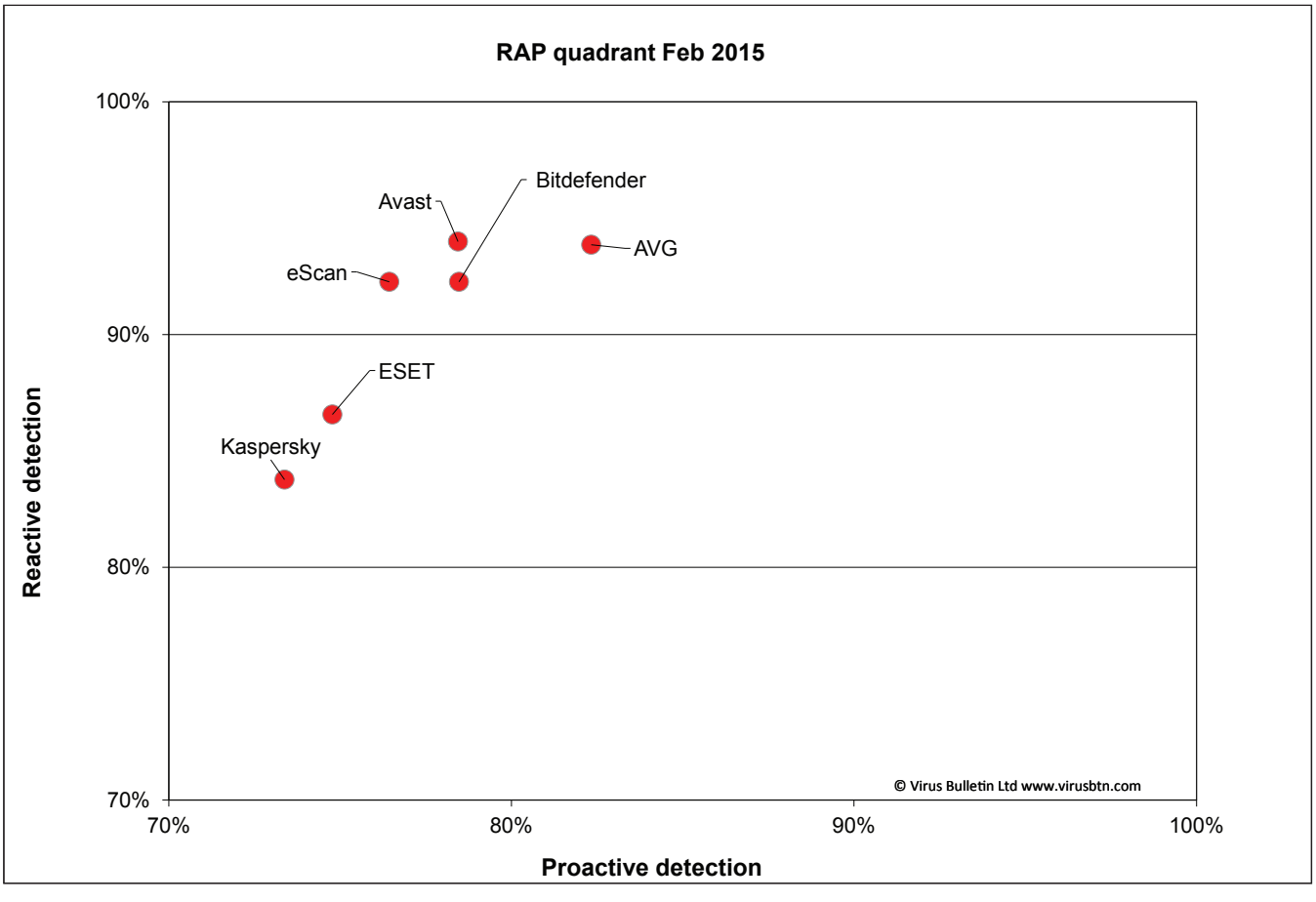

Standard activities - time increase
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Avast*
AVG
Bitdefender**
ESET
Kaspersky
* No on-read protection provided ** Measure exceeds chart area (Please refer to text for full product names.)

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
AVG	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Avast	OD	√	√	√	√	√	√	√	8	√	√	√
	OA	√	√	√	√	√	√	√	7	√	√	√
Bitdefender	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
eScan	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	√	√	8	8	√	√	√	8	√	√	√
ESET	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/5	X/√	X/√	√
Kaspersky	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	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.)

Reactive and Proactive (RAP) tests	VB100	Reactive		Proactive		Reactive average	Proactive average	Weighted average‡
		Set -2*	Set -1*	Set +1†	Set +2†			
Avast	VB100	94.11%	93.88%	81.37%	75.51%	94.00%	78.44%	88.81%
AVG	VB100	94.01%	93.72%	87.62%	77.04%	93.86%	82.33%	90.02%
Bitdefender	VB100	93.45%	91.09%	82.50%	74.43%	92.27%	78.47%	87.67%
eScan	VB100	92.36%	92.17%	80.18%	72.68%	92.27%	76.43%	86.99%
ESET	VB100	85.90%	87.22%	81.97%	67.58%	86.56%	74.78%	82.63%
Kaspersky	VB100	88.72%	78.82%	78.22%	68.53%	83.77%	73.38%	80.30%

*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.)



Product information	Install time (m)*	Reboot required	Third-party engine technology	Stability score	Stability rating
Avast	4	No		2.5	***Stable***
AVG	4	No		0	**Solid**
Bitdefender	3	No		2.5	***Stable***
eScan	6	No	Bitdefender	12.5	***Fair***
ESET	5	No		0	**Solid**
Kaspersky	9	No		1	***Stable***

** Install time includes initial updates and time to enable on-access protection (assuming reasonable typing speed and familiarity with product operation)*

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

(Please refer to text for full product names.)