COMPARATIVE REVIEW

RED HAT ENTERPRISE LINUX 5.2

John Hawes

Once again our annual visit to the *Linux* platform has rolled around. The relatively small number of participants in this month's test is in part due to the limited number of vendors that provide support for the platform, but has been further reduced by the unexpected withdrawal from the test of several of our regulars. Reasons given for sitting this one out included ongoing engine update work, difficulties coping with a deadline close to the new year, and a simple lack of organization in preparing a product for submission. However, past experience has taught us that any time saving introduced by having a diminished field of competition can be more than outweighed by the additional complexities introduced by the *Linux* platform. Based on my previous visits to the platform and the acidic comments of past reviewers, we expected problems with recalcitrant, opaque and poorly documented products as well as unexpected dependencies and incompatibilities.

More significantly, this month's comparative review sees the introduction of a new set of test results to our battery of additional data. Our RAP (Reactive and Proactive) testing setup, developed over the last few months and presented to the industry at last year's *VB* conference in Ottawa, makes its debut in these pages, and should provide some interesting insights into the products' performance. Its full value will, we hope, emerge in the long term, as further refinements are made and long-term trends are analysed – the new system and the intentions behind it are discussed in more detail on page 15.

PLATFORM AND TEST SETS

The last VB100 on *Red Hat Linux* was in 2006 (see *VB*, April 2006, p.13), until which time it had dominated the *Linux* slot in the comparative schedule for several years. Past reviewers tended to focus on the freely available and hugely popular *Red Hat* 9, the last version of which was released before the split between *Red Hat* and *Fedora*. In the intervening years, while we have turned our attention to commercial arch-rival *Novell/SuSE* (see *VB*, April 2007, p.11) and the more freely available *Ubuntu* (see *VB*, June 2008, p.16), *Red Hat* has continued down commercial lines, producing a line of business-focused distributions backed up by broad support offerings. These continue to hold a strong position in the blossoming market for open-source operating systems in business, while hobbyists and home-users alike have formed great attachments to the *Fedora* variant. The latest iteration of the commercial product, *RHEL 5.2*, was released in mid-2008, and while a further update to the 'Tikanga' line, version 5.3, was due for release halfway through this month's test, it seemed appropriate to stick with the edition most likely to be in use in *Red Hat*-based enterprises.

Installation and setup of the test systems was relatively straightforward at first. Following the simple and unfussy installer interface through and selecting the defaults as far as possible proved a simple and trouble-free task, and the GUI presented once up and running was equally free from excess glitter. The look and feel seemed fairly plain and clunky next to the beauty of the latest generation of desktops, but as a serious and sensible desktop for a server admin, it seems fit for purpose. Numerous graphical sysadmin tools are provided for those not keen on getting their hands dirty meddling with configuration files, and after some time finding our way around the anomalies and eccentricities of the system layout, things were mostly as we wanted them.

A few initial annoyances presented themselves, not least of which was the complete absence of NTFS support in the standard installation. As the test machines carry an NTFS partition hosting a number of useful lab items, some extra installation and configuration work was required – but nothing too taxing. Configuring the *Samba* daemon to make a storage area on each test system visible to *Windows* was also a fairly simple task. A separate system was positioned alongside the standard test machines for the purposes of the on-access tests. The system was running a basic *Windows XP Pro SP3* setup with the samba share from each of the test systems mounted. This would represent our client machine, accessing network resources and, hopefully, being protected from anything malicious which might be lurking on shared storage. Tests from here would include speed tests, which would be run separately with minimal network activity, to reduce the impact of additional traffic on the speed measurements.

The final stage of preparing the systems was to provide the open-source file-hooking module *dazuko*, which we knew from experience would be required by many products for their on-access scanning. As in previous *Linux* comparatives, getting this up and running proved less straightforward than was suggested by the accompanying documentation. The default kernel included with the operating system had a built-in module which turned out to be incompatible with *dazuko*. As a result, the kernel had to be recompiled without the module – which was by no means an arduous task, but certainly a time-consuming one. For the purposes of the test we simply made the alternative kernel and module available from the start, but this extra labour would have to be counted against those products using the system as far as ease of setup was concerned.

On-demand detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Alwil avast!	0	100.00%	1	99.95%	20	97.02%	64	98.20%	0	0
Avira AntiVir/Linux	0	100.00%	0	100.00%	0	100.00%	301	91.44%	0	0
ESET Security	0	100.00%	0	100.00%	0	100.00%	458	87.01%	0	0
Frisk F-PROT AntiVirus	0	100.00%	0	100.00%	174	96.08%	986	72.04%	1	0
F-Secure Linux Security	0	100.00%	1	99.95%	78	99.47%	458	86.99%	0	1
Kaspersky Anti-Virus	0	100.00%	0	100.00%	72	99.56%	464	86.83%	0	0
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	568	83.89%	1	0
Quick Heal for Linux	0	100.00%	48	97.43%	914	87.22%	717	79.67%	0	0
Sophos Anti-Virus	0	100.00%	2	99.97%	725	91.13%	562	84.06%	0	0
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	671	80.97%	0	0
VirusBuster SambaShield	0	100.00%	2	99.96%	757	81.43%	1369	61.17%	0	0

Next, the test systems were loaded with the test sets. The core detection set, based on the November 2008 WildList, had moved on considerably since the previous test, with large numbers of long-term residents finally evicted, including the bulk of the W32/Mytob, W32/Sdbot, W32/Rbot, W32/Stration (aka Warezov) and other worms which had dominated the list for several years.

Also falling off the list were the last of the W32/Virut polymorphic file-infecting viruses which had caused a considerable stir since their appearance last year. This left the list pretty devoid of genuine viruses and made up mostly of banking and online gaming password stealers. Many of the retired items which continue to show up in small numbers in our prevalence reports were moved temporarily across to our worms and bots test set. We hope, in future, to replace the worms and bots test set entirely for each new test, in the same manner as the trojan set – which, once again, was compiled from items seen in the few months prior to the test, and categorized into prevalent family groups.

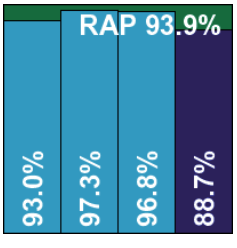
Still more recent items were put into the sets for the new RAP test. With the test deadline set for 7 January, the three 'reactive' sets were compiled from samples first seen in the last two weeks of 2008 and the first week of 2009, with the 'week +1' set compiled using samples seen in the week following product submission. Perhaps due to the change of year and various holidays upsetting the routines of both malware creators and external sample sources, the sets varied considerably over this period in both size and content type. After filtering, the final week's test set contained rather fewer samples than we had hoped, but still enough to give a reasonable reflection of detection abilities. Any anomalies caused by the makeup of the sets should be evened out over time – as with VB100 results, readers should not place too much importance on a single set of RAP results, but wait for true patterns to emerge as the tests are repeated over time.

Finally, the clean sets went through their usual tidying and expansion, with a fairly large selection of new samples added. New additions included the contents of a batch of cover CDs from technical magazines and a selection of packages broadly categorized as web-browsing and media manipulation tools. Although the expansion of this set was limited due to the amount of time devoted to preparing the other sets (and by a well-earned December break), the new additions seemed likely to challenge products coming up against our strict no-false-positives rule.

With all of the test collections in place, it was time to start feeling our way, with great caution, around the selection of products submitted for review.

Alwil avast! 3.1.5

ItW	100.00%	**Polymorphic**	97.02%
ItW (o/a)	100.00%	**Trojans**	98.20%
Worms & bots	99.95%	**False positives**	0



Alwil's *avast!* product for *Linux* arrived as a trio of RPM packages, one of which included an attempt to adjust the crontab scheduler to automate updates. This seemed to be taking some time, so was aborted, but some initial tinkering with the product found it still to be inactive. The instructions provided by the developers revealed that this was not the result of our impatience, but rather the requirement for a licence file, provided along with the submission but which needed to be copied

On-access detection	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Alwil avast!	0	100.00%	1	99.95%	20	97.02%	64	98.20%	0	0
Avira AntiVir/Linux	0	100.00%	0	100.00%	0	100.00%	301	91.44%	0	0
ESET Security	0	100.00%	0	100.00%	0	100.00%	468	86.72%	0	0
Frisk F-PROT AntiVirus	0	100.00%	0	100.00%	174	96.08%	986	72.04%	1	0
F-Secure Linux Security	0	100.00%	1	99.95%	428	99.56%	537	84.77%	0	1
Kaspersky Anti-Virus	0	100.00%	0	100.00%	500	96.97%	591	83.24%	0	0
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	568	83.89%	1	0
Quick Heal for Linux	0	100.00%	48	97.43%	914	87.22%	1466	58.42%	0	0
Sophos Anti-Virus	0	100.00%	0	100.00%	725	91.13%	562	84.06%	0	0
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	754	78.62%	0	0
VirusBuster SambaShield	0	100.00%	2	99.96%	757	81.43%	1369	61.17%	0	0

manually into the appropriate location, as indicated by a configuration file.

With these initial tasks complete, running the product proved straightforward, with the syntax of the command-line scanner a little esoteric but clearly laid out in the accompanying instructions. On-access scanning was similarly straightforward to administer, via standard and lucid configuration files, and everything ran pretty smoothly. Scanning speeds were quite excellent, both on access and on demand, and detection rates at their usual exemplary level.

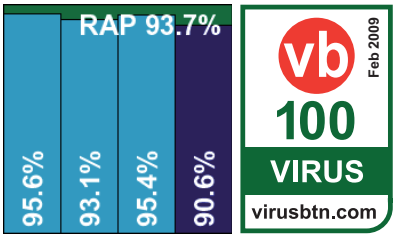
The RAP scores showed a slight dip in the earliest week – which, logically, one would expect to have the best coverage, but the coinciding holidays in many territories may have affected the throughput of labs in this period. More in tune with predictions, a second dip was observed in the 'week +1' set compiled after update freezing, but detection remained pretty solid over these likely unseen samples.

Getting back to the VB100 certification requirements, with no trouble at all handling the diminished WildList set and not a whisper of a false positive, *Alwil* takes the first VB100 award of 2009 with considerable style.

Avira AntiVir/Linux 2.1.12-101

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	91.44%
Worms & bots	100.00%	**False positives**	0

Avira's product came in the form of a single .tgz file. This raised some concerns initially, but on extracting, the file proved to contain an install script which performed all the necessary setup steps clearly and simply, with a series of simple questions allowing basic user configuration. With the locations of the licence file and *dazuko* module provided as part of the setup process (the *dazuko* module is developed and maintained by *Avira*), things were up and running in no time, and after perusing another well-documented, but again slightly eccentric set of command-line qualifiers, testing zipped along nicely.



Speed was highly impressive on demand, but on-access scanning seemed a little sluggish by comparison, and little difference was noted in speeds when archive scanning was activated (not the default setting). Indeed, it seemed the same kind of analysis was being performed – it took a considerable time to get through the control archive test set (consisting of the EICAR test file embedded at different depths inside a variety of archive formats) on access, without any detection being made, and not noticeably longer when full scanning was activated and access to the test files was correctly denied.

Detection rates were again superb, with over 90% across the board in all RAP sets including the 'week +1' set.

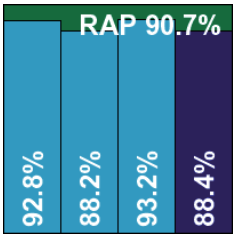
No detections were missed in the WildList set and no false alarms were generated in the clean sets, thus *Avira* starts 2009 with a VB100 award and great respect.

ESET Security for Linux 3.0.10

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	87.01%
Worms & bots	100.00%	**False positives**	0

On-demand throughput (MB/s)	Archive files				Binaries and system files				Media and documents				Other file types				Linux files			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)
Alwil avast!	364	8.37	564	5.40	230	11.30	236	10.99	86	24.06	98	21.13	93	10.11	98	9.65	511	1.85	530	1.78
Avira AntiVir/Linux	43	70.69	351	8.67	159	16.38	164	15.81	81	25.39	90	22.83	96	9.80	112	8.41	528	1.78	1623	0.58
ESET Security	631	4.82	631	4.82	414	6.27	414	6.27	71	29.16	71	29.16	92	10.28	92	10.28	1056	0.89	1056	0.89
Frisk F-PROT AntiVirus	308	9.87	309	9.83	400	6.49	436	5.96	69	29.98	100	20.57	74	12.68	109	8.67	393	2.40	806	1.17
F-Secure Linux Security	4577	0.66	4577	0.66	1110	2.34	1110	2.34	372	5.54	372	5.54	438	2.15	438	2.15	5610	0.17	5610	0.17
Kaspersky Anti-Virus	2471	1.23	2471	1.23	653	3.98	653	3.98	159	12.96	159	12.96	196	4.82	196	4.82	2561	0.37	2561	0.37
McAfee LinuxShield	718	4.24	718	4.24	435	5.97	435	5.97	84	24.57	84	24.57	105	8.97	105	8.97	1234	0.76	1234	0.76
Quick Heal for Linux	519	5.87	519	5.87	152	17.10	152	17.10	89	23.26	89	23.26	123	7.69	123	7.69	1452	0.65	1452	0.65
Sophos Anti-Virus	79	38.37	1302	2.34	314	8.28	337	7.71	65	31.59	103	20.12	31	30.24	134	7.06	283	3.33	2010	0.47
Symantec AntiVirus	158	19.28	NA	NA	213	12.21	213	12.21	128	16.11	128	16.11	97	9.67	97	9.67	802	1.17	NA	NA
VirusBuster SambaShield	382	7.96	643	4.73	243	10.68	246	10.56	255	8.09	181	11.42	128	7.35	148	6.36	1275	0.74	1638	0.58

ESET's long-standing dominance in VB100 testing has been challenged of late, both in terms of speed and detection rates, by some strong up-and-comers, with two of its most pressing rivals having already appeared in this month's review. Installation of the product was in the form of a single, straightforward RPM package, with control of the program via a centralized configuration file and thorough, well-documented options to the main binary. The default settings were pretty thorough, covering all file types and a wide set of archive types, and speeds in both modes were as excellent as experience has led us to expect.

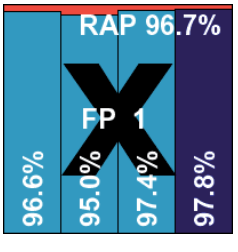


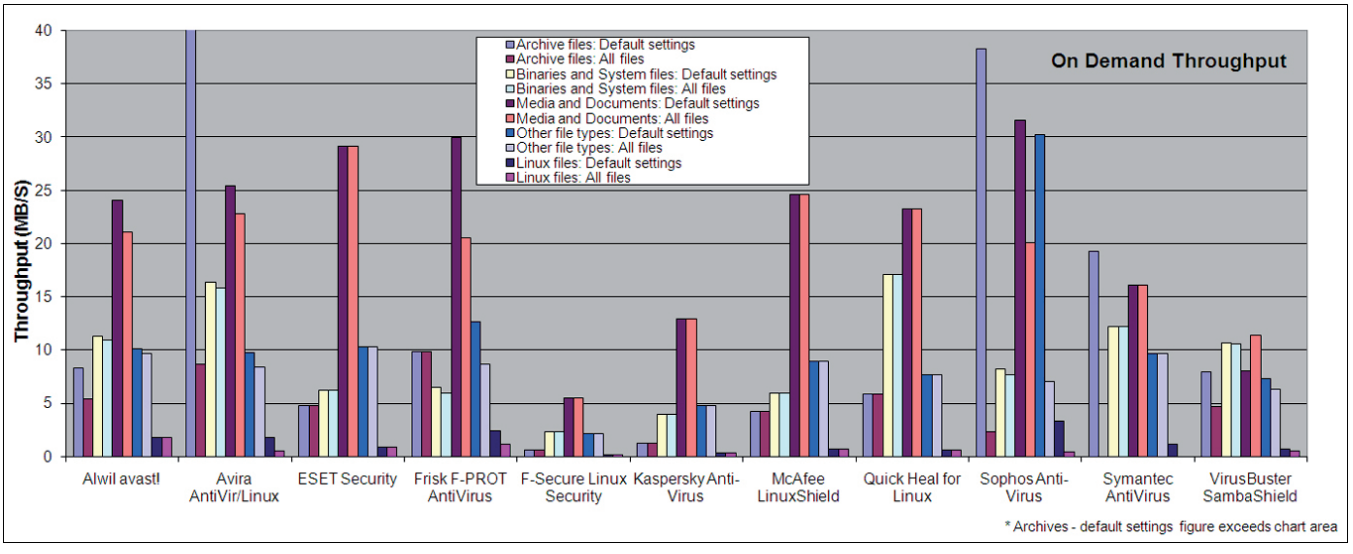
Detection rates were similarly strong – perhaps a fraction behind the excellent performers seen so far in the RAP tests, but close enough to put down to sample selection anomalies at this early stage. As usual for *ESET*, false positives were absent despite the product's strong heuristics, and the set of WildList samples presented no problems, thus *ESET* continues its excellent run of success with another VB100 award and a performance worthy of respect.

Frisk F-PROT AntiVirus for Linux 6.2.1.4252

ItW	100.00%	**Polymorphic**	96.08%
ItW (o/a)	100.00%	**Trojans**	72.04%
Worms & bots	100.00%	**False positives**	1

Frisk's *F-Prot* has shown itself in recent *Windows* comparatives to be the champion of pared-down, no-fuss protection, and here, once again, is an extremely basic piece of anti-malware kit – and none the worse for it. Installation consisted of little more than extracting an archive containing the required files, which could thus be located wherever the admin desires with relative ease. A simple install script is also provided to set up default paths to binaries and man pages. An initial problem was encountered when the submitted product turned out to be a simple workstation version with





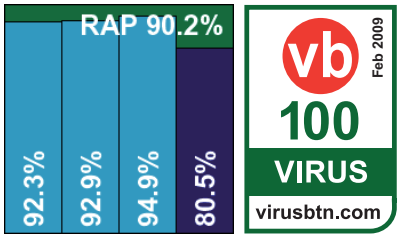
no on-access component. However, this issue was soon circumvented by grabbing the server version – available as a free trial download from the vendor's website – and snaffling the required on-access components for interaction with the *dazuko* module, which proved more than adequate to provide the full level of protection.

As expected, given the pared-down nature of the product, speeds and overheads were exemplary. Detection rates were decent across the three reactive RAP sets, and in the newest set quite remarkable, producing somewhat eye-opening results. Further investigation showed that a fair proportion of the detections recorded when parsing the results were in fact rather vague – many of them being labelled simply 'security risk' or even 'possible security risk'. Such detection labels would not be counted as false positives in the full test, so it was somewhat difficult to decide whether they should count as full detections in this case, but with time pressing and much of the processing of results already completed, we had no choice but to leave them in.

Moving on to the VB100 certification requirements, the WildList was once again covered without issues, but in the clean sets a single file from this month's addition of web browsers and associated tools was erroneously flagged as a backdoor. While there is potentially some scope for the item in question – a cookie management tool – to be abused, the alert was judged sufficient to deny *Frisk* a VB100 award this month despite the product's otherwise solid detection rates.

F-Secure Linux Security 7.02.73807

ItW	100.00%	**Polymorphic**	99.47%
ItW (o/a)	100.00%	**Trojans**	86.99%
Worms & bots	99.95%	**False positives**	0



F-Secure's product presented a much more professional aspect, with a .tgz file containing the required components alongside a thorough install script which leads the installer through all the required steps to get the product set up. This includes its own copy of the *dazuko* module – something which none of the other products so far have provided (despite requiring it for their on-access protection). It also comes with an attractive web-based interface, which plants its own desktop icon and provides configuration for much of the product. Along with numerous components in the init directory, a range of additional utilities are provided for the configuration and operation of the product, which provides a full protection suite, including firewall, alongside the standard anti-malware protection.

As expected, once the vagaries of the command-line interface had been decoded, helped along by clear documentation, detection rates were pretty solid, although less than perfect on some of the new families of polymorphic viruses. Scanning speeds were somewhat leisurely – which can partly be explained by the multiple engines in use by the product, which appear to contribute strongly to the depth of detection. Even using the default on-access settings, which ignored most archive types entirely, speeds were notably slower over the clean speed sets than for some of the other products. However, detection rates in the new RAP tests were once again excellent, with a notable dip in the 'week +1' set containing samples unlikely to have been seen by labs. For *Windows* users, *F-Secure* has

File access lag time (s/MB)	Archive files				Binaries and system files				Media and documents				Other file types				Linux files			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
Alwil avast!	629	0.20	629	0.20	284	0.09	284	0.09	242	0.08	242	0.08	176	0.12	176	0.12	1978	2.03	1978	2.03
Avira AntiVir/Linux	1973	0.65	1976	0.65	221	0.07	224	0.07	165	0.04	187	0.05	272	0.22	272	0.22	23430	24.80	2564	2.65
ESET Security	657	0.21	657	0.21	489	0.17	489	0.17	166	0.04	166	0.04	171	0.11	171	0.11	2019	2.07	2019	2.07
Frisk F-PROT AntiVirus	290	0.09	292	0.09	424	0.14	430	0.15	142	0.03	147	0.03	127	0.06	131	0.07	1469	1.49	2231	2.30
F-Secure Linux Security	234	0.07	4569	1.50	950	0.35	1147	0.42	355	0.13	415	0.16	408	0.36	462	0.42	1530	1.55	17443	18.44
Kaspersky Anti-Virus	74	0.02	2169	0.71	652	0.23	678	0.24	232	0.07	237	0.07	239	0.18	245	0.19	3146	3.27	3953	4.13
McAfee LinuxShield	592	0.19	592	0.19	609	0.22	609	0.22	235	0.07	235	0.07	228	0.17	228	0.17	2647	2.74	2647	2.74
Quick Heal for Linux	32	0.01	NA	NA	194	0.06	194	0.06	165	0.04	165	0.04	179	0.12	179	0.12	2480	2.56	2480	2.56
Sophos Anti-Virus	91	0.03	761	0.25	357	0.12	389	0.13	168	0.04	170	0.04	165	0.11	173	0.11	2486	2.57	2857	2.96
Symantec AntiVirus	163	0.05	NA	NA	253	0.08	253	0.08	196	0.05	196	0.05	156	0.10	156	0.10	1842	1.89	NA	NA
VirusBuster SambaShield	56	0.02	NA	NA	312	0.10	312	0.10	237	0.07	237	0.07	204	0.15	204	0.15	2590	2.68	NA	NA

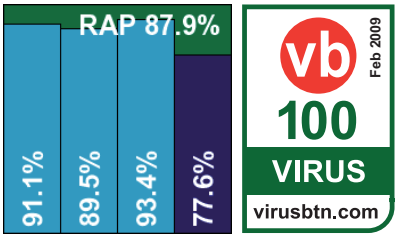
made much of its additional 'Deepguard' protection with additional cloud-based black- and whitelists (which we have yet to be able to properly test under the requirements of the VB100); whether this layer is available for *Linux* users was not made clear.

Overall, the product's performance was nothing to be sniffed at, with the WildList test set covered without a glitch, and the cleanliness of the clean sets was only called into question by a 'potentially unwanted' alert on the same file as was described as a backdoor by the *Frisk* product. As this is allowable under the VB100 rules, *F-Secure* earns a VB100 award, and extra praise for its solid and lucid design and usability.

Kaspersky Anti-Virus for Linux File Servers 5.7-26

ItW	100.00%	**Polymorphic**	99.56%
ItW (o/a)	100.00%	**Trojans**	86.83%
Worms & bots	100.00%	**False positives**	0

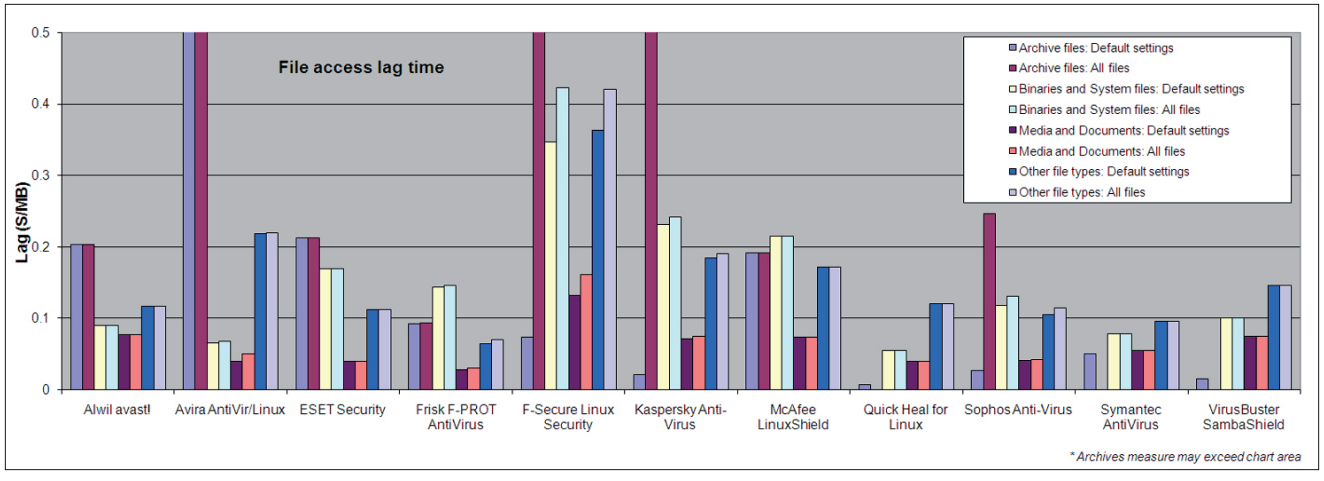
Kaspersky's *Linux* range has in the past eschewed the popular *dazuko* path in favour of the 'Samba vfs object' method, functioning only on file systems shared via *Samba*. In previous tests *Kaspersky* has proved to be one of the few vendors to utilize the technology to its full efficiency. This time, however, the vendor seems to have moved on to its own in-house technology, implementing full on-access detection without the need for any external software. Installation takes the form of an RPM, with a perl script to be run post installation to perform the necessary setup steps.



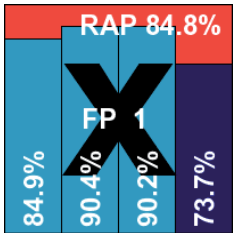
Operation of the product was less well streamlined, with lengthy commands needing to be issued from the command line and somewhat unpredictable syntax. Scanning speeds were not the fastest, but detection rates were at their usual solid level. The product showed another splendid performance in the RAP tests with, as was predicted for all products, a slight decline in the 'week +1' set. The diminutive WildList yet again presented no difficulties, and false positives were absent, thus earning *Kaspersky Lab* another VB100 award.

McAfee LinuxShield 1.5.1

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	83.89%
Worms & bots	100.00%	**False positives**	1



McAfee's *Linux* product has, in previous comparative reviews, reflected the company's reputation for professionalism and seriousness. Here, that impression was bolstered, with a broad collection of PDF-format documentation needing to be read before the required installation order of the RPM packages could be ascertained. This done, and after a standard array of installation questions, the product was quickly up and running, with administration performed via a fairly clear and thorough web interface.



A few changes have clearly taken place since my previous encounter with the product however, and a chink in the company's armour emerged when it became clear that these changes had yet to filter through to the online documentation, knowledgebase and even the staff submitting the product. The update method – admittedly not the standard online method, but one certain to be preferred by many *Linux* systems administrators who may be running their servers behind all kinds of protective barriers – had been adjusted with a recent iteration of the product, rendering previous techniques ineffectual and online instructions inaccurate. Eventually, after much discussion with tech support personnel, the problem was diagnosed and the correct form of updates provided, albeit not quite the freshest possible from the submission date. A more accurate set of instructions was also provided, and testing continued.

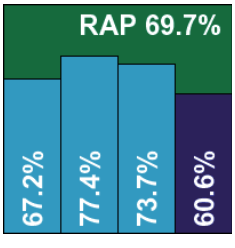
The running of on-demand scans required the use of the interface from which scan 'tasks' could be designed and run; these same tasks could also be kicked off from the command line, allowing for some scripting and the use of the standard cron scheduler. However, the lack of ability to configure the tasks from the bare console, even to the extent of providing a scan target, seemed a rather glaring omission which the diehard command-line-loving *Linux* administrator may find hard to forgive.

Once the scans were set up and run, scanning speeds were surprisingly good, overheads not too heavy, and detection rates in the standard test sets reached the expected level. In the RAP tests, scores were generally pretty good, with that telltale dip in the 'week +1' set demonstrating the superior performance of signature detections over heuristic and generic methods, but a worthy performance nevertheless. As far as certification requirements were concerned, nothing was missed in the WildList, but in the clean sets a single file – which has been included in the set since the summer of 2007 – was alerted on with a generic trojan identification, thus spoiling *McAfee*'s recent run of success and denying the vendor a VB100 on this occasion.

Quick Heal for Linux 10.00

ItW	100.00%	**Polymorphic**	87.22%
ItW (o/a)	100.00%	**Trojans**	79.67%
Worms & bots	97.43%	**False positives**	0

Quick Heal's product is another *dazuko*-based setup, with a nice, simple installer inside a .tgz file which, for once, utilizes colour to improve clarity and ease of use. With the setup completed quickly and easily, a proper desktop interface was another pleasant surprise, but although easy on the eye it provided little in the way of in-depth configuration. Some was available in more traditional configuration files, but even here some functions, such as enabling of archive scanning on access, seemed impossible.



		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
Alwil avast!	OD	X/√	X/√	√	X/√	X/√	√	√	X/√	√
	OA	√	√	√	√	√	√	√	√	√
Avira AntiVir/Linux	OD	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
ESET Security	OD	√	√	√	√	√	5	√	√	√
	OA	√	√	√	√	√	5	√	√	√
Frisk F-PROT	OD	X	5/√	5/√	√	5/√	5	5/√	5/√	√
	OA	1	5/√	5/√	X	5/√	2/5	5/√	5/√	√
F-Secure Linux Security	OD	√	6	6	6	6	3	6	6	√
	OA	X/√	X/√	X/√	X/√	X/√	X/5	X/√	X/√	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
McAfee LinuxShield	OD	√	√	√	√	√	√	√	√	√
	OA	2	√	√	√	√	√	√	√	√
Quick Heal AntiVirus	OD	2	√	√	X	√	1	√	X	√
	OA	2	X	X	X	X	X	X	X	√
Sophos Antivirus	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/√	X/√	X/√	X/√	X/8	X/√	X/8	√
Symantec AntiVirus	OD	X	X	3	3	3	1	3	3	√
	OA	X	X	3	3	3	1	3	3	√
VirusBuster Sambashield	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√

Key:

X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

*Executable file with randomly chosen extension

X/√ - Default settings/thorough settings

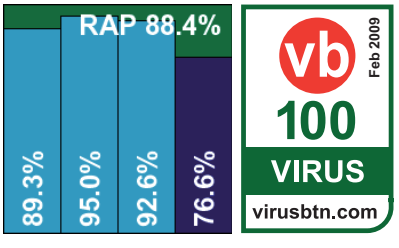
[1-9] - Archives scanned to limited depth

Of course, all of this helped with *Quick Heal*'s famous speediness, which was once again up there with the best. Although detection rates were a little behind the best scores recorded so far in this review, in most sets they were decent, and the WildList presented no problems. With no false positives either, *Quick Heal* reaches the required standard and earns another VB100 award.

Sophos Anti-Virus for Linux 6.4.5

ItW	100.00%	**Polymorphic**	91.13%
ItW (o/a)	100.00%	**Trojans**	84.06%
Worms & bots	99.97%	**False positives**	0

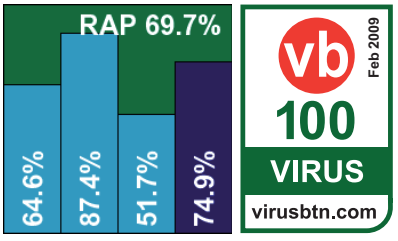
Another company with a solid reputation in the enterprise market, *Sophos* also ignores the availability of the *dazuko* module and goes for its own in-house technology to provide on-access scanning. The product installs simply and smoothly on this platform, which is a prime target as one of the leading *Linux* setups in use in enterprise. The absence of any recompilation, dependencies or other fiddly tasks counts strongly in the product's favour as far as initial installation goes. Post-install operation is also something of a breeze, with a well-documented and pleasantly usable product. Alongside the standard command-line operation and configuration files, another web interface is provided, which, again, is very well laid out and simple to use.



Scanning speeds were similarly pleasing, particularly with the default settings, and lag times were among the best on offer. Detection rates across all test sets left little to be desired, with a few misses in the polymorphic and trojan sets more than made up for by an excellent showing across the new RAP sets, although the dip in the 'week +1' set was perhaps a little more pronounced here than elsewhere. With no false positive issues and nothing missed in the WildList set, *Sophos* comfortably achieves a VB100 award.

Symantec AntiVirus for Linux 1.0.7.14

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	80.97%
Worms & bots	100.00%	**False positives**	0



Somewhere in the deeper circles lies a special hell, where testers who have devoted their lives to the more unforgiveable sins must forever wrestle fruitlessly with the *Symantec Linux* product. After two previous encounters with the product, and despite being given some insight into its intricacies by a gifted support engineer, it remains opaque and bizarre. The company's support forums are littered with desperate cries for help and simple requests for an explanation of the Machiavellian layout of the configuration process, while the accompanying documentation provides only the vaguest outline of how the controls actually work.

For those happy to go with the defaults, perhaps things are not so bad. The install process consists of a batch of RPM packages along with setup instructions buried in a PDF, and once these have been followed the product is quickly up and running. An interface is even provided, but here there is little more than a summary of the product's version information and running status, as well as a button marked 'update'. Manual updating is also possible, with the definitions provided in the form of a self-extracting install file. On the test platform, this required several extra packages to be installed to support its extraction processes, but with these tasks carried out it worked without a hitch. The product was rendered fully operational, including the on-access scanning provided by the company's own technology, fairly easily.

It is only when the default settings must be changed that things become difficult. The configuration is not stored, as is standard in Unix/*Linux*, in a nice, humanly readable and easily adjusted configuration file. Instead, a database in the style of the *Windows* registry is used, and any changes must be passed into this using a dedicated configuration tool. This tool responds equally blankly to both accurate and errant attempts to render the lengthy, syntactically complex commands required. Frequent rechecking of the full list is a must to ensure the proper changes have been made, while documentation of the numerical codes representing such options as on-detection actions seems non-existent.

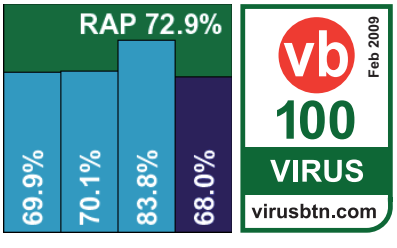
With the required tweaks assumed to have been made, the process of running command-line scans is a little less arduous, but by no means straightforward, and is similarly lacking in any form of feedback from the product. An option was found which would at least retain control of the command line, returning it when the scan completed, which enabled speed tests and monitoring of progress without recourse to checking the logging. This took the form of complex, barely readable output via the syslog facility, and in the main proved sufficiently usable to produce the required results.

In the RAP tests, eccentric and uneven figures hinted at a possible error in the multi-stage process of extracting information from the multi-record-per-line confusion of the logs, and a retry did produce different, but similarly erratic, results. In a slight bending of the VB100 'three attempts' rule, the scan was run multiple times and detections for each scan, varying by up to 10% each time, merged together to produce the final figures displayed here. It seems more than likely that this may not reflect the true detection capabilities of the product – for which I can only apologize to the vendor, but it was the best that could be achieved under the trying circumstances. If a more accurate way of procuring results can be found, we will strive to achieve it and update these figures – watch this space.

On a happier note, scanning speeds were pretty good and detection rates in the standard sets very good, with no difficulty handling the WildList and no false positives; a VB100 is duly awarded.

VirusBuster SambaShield 1.2.018-1.2.1.7

ItW	100.00%	**Polymorphic**	81.43%
ItW (o/a)	100.00%	**Trojans**	61.17%
Worms & bots	99.96%	**False positives**	0



The final product on the test bench brings what I had expected, based on past experience, to be the main rival to the *dazuko* setup in terms of on-access file-hooking: the Samba vfs object. *VirusBuster*'s product provides a series of .tgz files with an install script, making the installation reasonably straightforward despite a few rather vague passages of text. The setup of the *Samba* protection must be done manually, with instructions provided, but a slight inaccuracy in the guidelines led to the *Samba* share in question being rendered completely inaccessible – safe from malware perhaps, but hardly the ticket. A small tweak soon had things operational however, and testing continued.

Scanning speeds were fairly decent, and overheads pretty good too, but detection rates lagged a little behind this

month's very strong field. Logging proved a particular issue, with complex multi-line logs not the most comfortable to parse – for *Linux* administrators with large amounts of text-based data to handle, such inelegancies weigh heavily, just as they do for testers. However, after a period of hair-pulling and text-mangling, usable results were obtained, showing some fairly decent scores in the RAP sets, which improved considerably when the non-default 'grayware' option was enabled. Moving on to the VB100 certification requirements, the WildList was once again covered thoroughly and with no false alarms generated in the clean test set, *VirusBuster* is awarded a VB100.

CONCLUSIONS

The *Linux* test is always a bit of a roller-coaster of delight and despair, and here both highs and lows were very much in evidence. Some products were well designed, sensibly laid out and clearly documented, while others seemed to go out of their way to be obtuse, awkward and uncooperative. Nevertheless, most were somehow wrangled into line and useful results obtained, with on-access problems – once a major difficulty under *Linux* and the cause of many failures – put firmly in the past. All the products here managed to provide their on-access functionality smoothly and, for the most part, efficiently.

Performance is a significant issue, and in past *Linux* tests we have seen wide variations in scanning times and overheads, particularly between products using the same method to handle file access hooking. However, this again seems a thing of the past, with the gap between the faster and slower products narrowing.

Of course, the speed results depend a lot on the depth of scanning on offer and on the variety of file and archive types being analysed, and this is why we provide the additional archive table and scanning speeds for both default and full modes. With command-line products we often expect the default setting either to be everything off or everything on, but the trend was bucked this month with a wide variety of default settings, from thorough scanning with automatic disinfection or removal, through to fast and light scanning with reporting only. What guidance was available, in the form of usage notes, man pages and full manuals, generally required thorough reading before any assumptions could be made about the product's operation.

The limited number of updates to the WildList made for a fairly easy month for our small field of competitors, with none of them in any way troubled by the contents of the list. Hopes of a full set of VB100 awards were dashed, however, by a couple of unlucky false positives from otherwise high-performing products.

Of course, of interest to many this month will be the first set of results from our RAP testing. These figures conformed largely with our expectations. The extent of the decrease in detection seen in the 'week +1' results gives a reasonable indication of which products are using strong heuristic and generic detection, and which rely more heavily on fast response to new sightings.

The RAP results include some anomalous figures, not least in the earliest batch of samples, which many products fared less well against than those seen more recently. One explanation may be the coincidence of public holidays with that week of sample gathering, and the possibility that depleted labs may not have processed quite as much as usual. Other problems included a couple of products with logging and classification complications, which highlight the need to further refine the system and to define the rules of engagement more precisely. Further improvements are also planned to the back end of the set-up, including sample selection, automated validation procedures and so on, and we hope that the build-up of results over time will show some interesting trends and patterns.

Normally in this spot it would be my duty to point out that this type of static scanning does not fully reflect the overall capabilities of the product, as additional functionality may provide an extra layer of protection. On the desktop this is, of course, true, with a range of additional barriers being added to the latest generations of products. On file servers and at gateways however, the static scanning engine remains king, and detection rates, along with speed, usability and other factors looked at here, will continue to be the prime measure of product performance. We hope the latest addition to the information provided here helps give our readers some deeper insight into these factors.

Technical details

All products were tested on identical systems with *AMD Athlon64* X2 Dual Core 5200+ processors, 2 GB RAM, dual 80GB and 400GB hard drives, running *Red Hat Enterprise Linux 5.2*.

On-access tests were run from an AMD Sempron 3000+, 1.79GHz client with 512MB RAM, running *Microsoft Windows XP SP3*, connected via 100MB/s networking and *Samba* version 3.0.28-1.

Any developers interested in submitting products for VB's comparative reviews 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.