COMPARATIVE REVIEW

UBUNTU LINUX 8.04LTS SERVER EDITION

John Hawes

Once again the VB100 review rolls around to its annual visit to a *Linux* platform, and once again the same questions arise. The ever-growing hordes of *Linux* and open-source aficionados continue to revel in the relative impenetrability of their security model and in the scant attention paid to them by malware creators. Why, I am asked on what seems like a daily basis, would I want to run anti-virus on my *Linux* box? What have I to fear? A tiny handful of malware with puny penetration levels is surely a risk worth taking, runs the standard argument.

Of course, this is quite beside the point; while *Linux* as a desktop operating system continues to nurture its small, but generally keen and committed user base, it is when running on a server that it is really at home, continuing to dominate at gateways and scattered throughout corporate and academic networks. Fileserver systems, with their arrays of *Windows* clients storing and transferring all manner of things thanks to the delights of *Samba*, can be nasty breeding grounds for network-wide malware infestations if they are not properly protected. However, they can also be used as effective blockades, preventing malicious code from being passed to new targets. Even where desktops feature their own anti-malware systems, corporate policies often (rightly) insist on thorough regimes of protection with no system allowed to operate without malware scanning, no matter how secure it may seem. For this reason, the *Linux* VB100 generates a great deal of interest from our readers in the corporate world, who are not above demanding tests on far more esoteric platforms.

Ubuntu Linux is a relative newcomer to the scene compared to the likes of *SUSE* and *Red Hat*, the even more venerable *Slackware* and, of course, *Debian*, from which *Ubuntu* evolved. The distribution's first release was in 2004, and since then it has seen massive growth, with strong financial backing through its links to *Canonical Ltd* and its entrepreneur founder Mark Shuttleworth, the first African to venture into space.

Ubuntu has shied away from the duality of commercial and free versions adopted by other big-money distros, and embraced the open-source philosophy wholeheartedly. Accompanied by numerous offshoot projects focusing on specific desktops systems and user groups, *Ubuntu*'s focus on friendly usability, stability and consistent updating has brought strong penetration of desktops – a poll held last summer found over 30% of respondents were using it, with its nearest rival, *OpenSUSE*, at 19% and *Debian* at 11%. At the server level fewer details are available, but the server edition seemed more appropriate to our purposes; of course this selection brought with it the likelihood of some compromises in usability, with any cuddly ease of use likely to have been stripped away in favour of efficiency, security and robustness.

The challenge of learning a new platform should, I hoped, be somewhat mitigated by the fairly small number of entries this month – a mere 15 products providing a relatively easy ride between the mammoth *Vista* test last time around and what is likely to be an even more gargantuan array of products in the *XP* test scheduled to take place later in the summer. Looking forward to simple command-line interfaces providing easy access to configuration options, I burned the install image, dusted off my rather neglected *Linux* skills, and ventured bravely into the lab.

PLATFORM AND TEST SETS

Installation of *Ubuntu* was a pretty straightforward process, guided by a pleasant graphical setup process. As usual in VB100 testing I tried to keep things as simple as possible, sticking to the default settings to get as close as possible to an out-of-the-box setup. Of course this policy couldn't be applied perfectly, with some stages such as disk partitioning requiring specific tuning for my needs, but the final setup provided the basic *Ubuntu* fileserver. As expected, this didn't include a desktop environment, so those products with attractive interfaces would not have their full range of offerings investigated, but the command-line style is generally preferred at the server level anyway, with a minimum of 'magic' going on to open potential security holes and drain resources.

Less expected was the absence of other useful items, including an NFS implementation, but a little investigation showed that a large range of extra goodies were available on the install CD. Beyond a few basic steps such as configuring networking, connecting to the lab servers and client systems and copying test samples to the local machines, very little further work was required before taking snapshot images and getting down to business. In the previous *Linux* test (see *VB*, April 2007, p.11) a copy of *dazuko*, the open-source file-hooking software used by many *Linux* products, was prepared on the test machines in advance, but in this case one of the submissions had thoughtfully included a pre-built binary so this step was not necessary (although I had little doubt that some compilation would eventually be required).

Client systems were also prepared, using a standard *Windows XP SP2* image with the *Samba* shares of the test

On-demand detection rates	WildList viruses		Worms & bots		File infector viruses		Polymorphic viruses		Linux samples		Legacy samples		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Alwil avast!	0	100.00%	0	100.00%	0	100.00%	319	87.13%	2	96.67%	1027	97.02%	2	
AVG Anti-Virus	0	100.00%	1	99.94%	7	98.43%	691	73.89%	3	88.33%	710	95.83%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	6	66.67%	0	100.00%		
BitDefender Security	0	100.00%	0	100.00%	2	98.95%	0	100.00%	4	93.33%	9	99.93%		
Doctor Web Dr.Web	16	97.55%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	12
ESET Security	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	
F-Secure Linux Security	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	
MicroWorld eScan	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	3
Norman Virus Control	0	100.00%	0	100.00%	7	99.15%	765	73.47%	0	100.00%	269	99.00%		
Quick Heal	0	100.00%	1	99.87%	9	98.43%	808	83.86%	7	66.67%	1127	93.95%	2	
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	7	65.00%	0	100.00%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
VirusBuster SambaShield	0	100.00%	2	99.91%	8	99.21%	224	79.29%	6	83.33%	20	99.92%		

servers mapped, with all on-access tests planned to be run from these. To avoid unfairness, network activity was kept to a minimum during the tests, which were run one at a time to further reduce the possibility of unequal treatment.

The test sets were aligned with the March 2008 WildList, which was released a few weeks prior to the test set deadline of 2 May and the product submission deadline of 5 May. The latest WildList included a fairly large number of new additions, but these were concentrated in a few families – most notably a large swathe of W32/OnlineGames trojans, showing further evolution of the WildList into the cybercrime-ridden modern world. Quite a few older items fell from the list, including several strains of W32/Mytob and W32/MyDoom, and also the veteran W32/Nimda, which finally dropped off the list after a marathon stint of officially being in the wild.

My attendance of numerous meetings and conferences this month hampered any efforts to expand the other test sets by more than a minimal amount, with only a handful of items added to the clean and infected sets and the meagre set of *Linux* samples dusted off. The most significant addition was the insertion of a set of *Linux* files into the clean set, to form an extra part of the speed measurements. This time the samples were taken from a separate system from those running the tests, one which had been in heavy use for some time and thus held a more eclectic range of items. The entire contents of /bin, /sbin, /etc and /opt were included, making the new set on a par with the others in terms of size on disk, but considerably ahead of them in the number of files it contained.

Finally, the standard archive test set consisted of the EICAR test file embedded in a selection of archive types at a range of depths. These would, as usual, be scanned with the default settings and with 'all files' and 'scan archives' settings enabled where possible, and detection at a depth of five or more levels on at least half of the set would be considered adequate for a product's inclusion in the full archive graphs. With everything ready to go, it was time to see how the selection of products fared.

Alwil avast! for Linux 3.1.0

ItW	100.00%	**Polymorphic**	87.13%
ItW (o/a)	100.00%	**Linux**	96.67%
Worms & bots	100.00%	**Legacy**	97.02%
File infectors	100.00%	**False positives**	2

Alwil's product arrived as several archive files, which when unpacked were found to contain simple installer scripts which did all the work of setting things up very

On-access detection rates	WildList viruses		Worms & bots		File infector viruses		Polymorphic viruses		Linux samples		Legacy samples		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Alwil avast!	0	100.00%	0	100.00%	0	100.00%	319	87.13%	2	96.67%	1027	97.02%	2	
AVG Anti-Virus	0	100.00%	1	99.94%	7	98.43%	691	73.89%	6	71.67%	710	95.83%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	93.33%	0	100.00%		
BitDefender Security	0	100.00%	0	100.00%	2	98.95%	0	100.00%	4	93.33%	9	99.93%		
Doctor Web Dr.Web	16	97.55%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	12
ESET Security	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	
F-Secure Linux Security	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	
MicroWorld eScan	0	100.00%	0	100.00%	0	100.00%	1	99.88%	0	100.00%	0	100.00%	1	3
Norman Virus Control	0	100.00%	0	100.00%	7	99.15%	916	66.94%	6	66.67%	269	99.00%		
Quick Heal	0	100.00%	1	99.87%	9	98.43%	808	83.86%	7	66.67%	1173	93.00%	2	
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.95%		
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
VirusBuster SambaShield	0	100.00%	2	99.91%	8	99.21%	224	79.29%	8	70.00%	20	99.92%		

nicely. However, the on-access component was a little less straightforward – it needed some compilation and access to the *dazuko* sources, which caused a headache and required calls to the developers for advice as the various requisites were set up. The libdazuko library, not built by default by the standard setup process, was also needed, but when at last everything was in place testing proceeded without further incident. Configuration, both of the command-line scanner and the on-access components, operated in a straightforward and standard fashion, with ample documentation available to guide the novice user.

Scanning speeds were about what I should have expected, my hopes of seeing testing times cut drastically as a result of using a pared-down operating system having quickly been dashed. On-access scanning speeds in particular were somewhat slower than I had hoped, doubtless due in large part to the test being run across the network. *Avast!*'s detection rates were little changed from previous tests, although detection for the single file-infector on the WildList which was missed last time around was added and the core set was covered without problems.

In the clean sets, however, a couple of items were mislabelled as malware, including one which has tripped up a series of products in the past year, and thus *Alwil* will have to wait a little longer before reclaiming its place on the VB100 podium.

AVG Anti-Virus 7.5.51

ItW	100.00%	**Polymorphic**	73.89%
ItW (o/a)	100.00%	**Linux**	88.33%
Worms & bots	99.94%	**Legacy**	95.83%
File infectors	98.43%	**False positives**	0

AVG's product was considerably simpler to install, coming as a single .deb installer package which set everything up in a few moments, the majority of which were spent entering a licence key. Again using the *dazuko* file-hooking system, this time all the installer required was the kernel module to be in place. The design conformed to *Linux* norms, with straightforward syntax to the command-line scanner and the configuration files for the on-access monitor. Guidance and information was also ample and properly implemented.

Speeds were a little disappointing, even more so with scanning of all files and archives enabled, but detection

On-demand throughput	Archive Files				Binaries and System Files				Linux Files				Media and Documents				Other File Types			
	Default Settings		All Files		Default Settings		All Files		Default Settings		All Files		Default Settings		All Files		Default Settings		All Files	
	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Through-put (MB/s)
Alwil avast!	980	3.77	980	3.77	554	6.77	554	6.77	856	2.16	856	2.16	158	11.37	158	11.37	143	6.49	143	6.49
AVG Anti-Virus	2822	1.31	2910	1.27	832	4.51	1518	2.47	3638	0.51	5846	0.32	399	4.49	410	4.37	439	2.11	560	1.65
Avira AntiVir	57	64.31	751	4.92	276	13.58	290	12.91	2078	0.89	2362	0.78	159	11.28	160	11.19	165	5.62	166	5.57
BitDefender Security	1599	2.31	1599	2.31	612	6.12	612	6.12	1240	1.49	1240	1.49	163	11.00	163	11.00	183	5.06	183	5.06
Doctor Web Dr.Web	3739	0.99	3739	0.99	852	4.40	852	4.40	1576	1.17	1576	1.17	196	9.12	196	9.12	223	4.16	223	4.16
ESET Security	1110	3.33	1110	3.33	850	4.41	850	4.41	772	2.39	772	2.39	111	16.15	111	16.15	123	7.53	123	7.53
Frisk F-PROT	539	6.86	539	6.86	847	4.42	847	4.42	627	2.94	627	2.94	106	16.94	106	16.94	110	8.38	110	8.38
F-Secure Linux Security	4307	0.86	4307	0.86	975	3.84	975	3.84	2524	0.73	2524	0.73	323	5.54	323	5.54	345	2.69	345	2.69
Kaspersky Anti-Virus	3246	1.14	3246	1.14	685	5.48	685	5.48	1571	1.17	1571	1.17	188	9.52	188	9.52	207	4.46	207	4.46
MicroWorld eScan	4036	0.92	4036	0.92	615	6.09	615	6.09	2153	0.86	2153	0.86	256	6.99	256	6.99	275	3.36	275	3.36
Norman Virus Control	1228	3.01	1228	3.01	3335	1.12	3335	1.12	1697	1.09	1697	1.09	154	11.60	154	11.60	301	3.07	301	3.07
Quick Heal	957	3.86	957	3.86	187	20.04	187	20.04	1224	1.51	1224	1.51	135	13.29	135	13.29	106	8.69	106	8.69
Sophos Anti-Virus	61	60.13	2004	1.84	523	7.17	560	6.69	547	3.38	1476	1.25	99	18.14	194	9.24	63	14.62	249	3.71
Symantec AntiVirus	354	10.44	NA	NA	413	9.08	NA	NA	1351	1.37	NA	NA	198	9.05	NA	NA	211	4.38	NA	NA
VirusBuster SambaShield	345	10.72	346	10.69	524	7.15	524	7.15	621	2.97	621	2.97	102	17.63	102	17.63	104	8.91	104	8.91

rates were good, with no WildList samples missed and no false positives raised, and thus *AVG* earns a VB100 award.

Avira AntiVir for Linux 2.1.12-31

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	66.67%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	0

Avira developed the *dazuko* system and continues to fund its maintenance and development. It is not surprising, therefore, that the company's product is among those making use of the file-hooking software.

The installation setup came as an archive file containing an install script, as well as the pre-built *dazuko* module – I suspect this addition is not generally provided for customers, but many *Linux* distributions come with the binary package available. The installer offered the delights of centralized management systems and graphical interfaces, which I was forced to turn down, and again the design, settings and documentation were excellent.

Scanning speeds this time were a little more impressive, and once again detection rates were superb, with most of the missed items merely being the result of rare file types not being scanned with the default settings. With flawless coverage of the WildList and not a hint of a false positive, *Avira* easily qualifies for a VB100 award.

BitDefender Security for Linux 3.0.0.80505

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	93.33%
Worms & bots	100.00%	**Legacy**	99.93%
File infectors	98.95%	**False positives**	0

BitDefender's product was another using the .deb system, this time with a built-in installation system too. This caused some issues initially as older versions of C++ libraries were required, which in turn required the installation of several other dependencies. Presumably on a fully networked system this would all have been handled by the package manager, reaching out to the web for any requirements.

Once over these hurdles things went very easily however, with a *Samba* VFS module used for the on-access component – this was the standard alternative to the *dazuko* system in the last *Linux* test and its operation proved simple, with a small change to the *Samba* configuration to point it at the new scanning object the only requirement.

In the previous *Linux* test several products using the VFS method encountered difficulties with speed and stability, but there were no such issues here, with things running along at excellent speeds without so much as a wobble until on-demand scanning of the archive set brought up a few segmentation-fault crashes. A handful of items were removed and the test was completed successfully, and the issue could not be reproduced in isolation. Detection was excellent, and without any samples missed in the WildList set and avoiding false positives, *BitDefender* also wins another VB100 award.

Doctor Web Dr. Web for Linux 4.44.0

ItW	97.55%	**Polymorphic**	100.00%
ItW (o/a)	97.55%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	3

The *Dr.Web* product was a little more pared-down than the others, with a few simple .tgz archives which just needed extracting into the system root to drop their files into the right spots. After some teething problems with permissions – the result of inadequate perusal of the documentation on my part – things got trotting along nicely. I found the syntax of the command-line scanner a little quirky, but soon mastered it, along with the implementation of the on-access scanner SpIDerGuard, which again made use of *Samba*'s built-in VFS objects system.

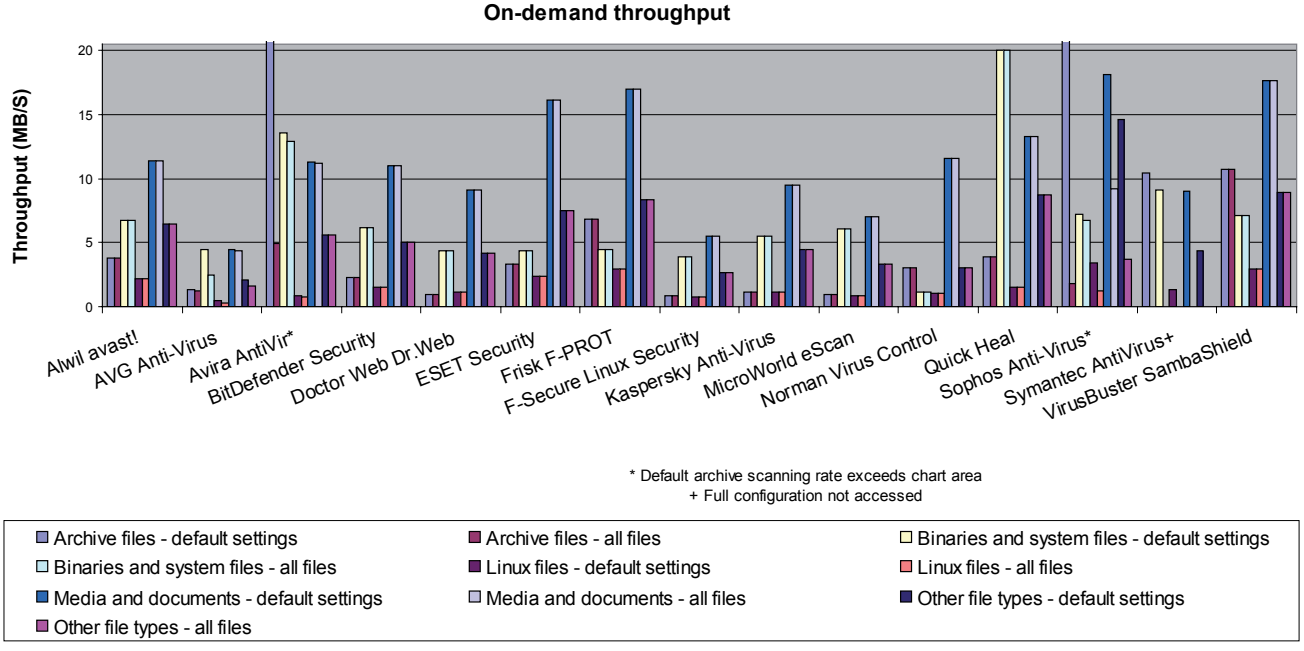
The product's extreme thoroughness in analysing archives meant that scan times on some sets were rather long, but hugely detailed logs were produced, packed with information on the files which had been scanned. These included alerts on a range of 'riskware' and 'hacktool' products which I may not have wanted to have around had I been a genuine network administrator.

On more normal files speeds were very impressive, and detection rates were also extremely high, but once again a handful of items from the WildList set were not covered, and a couple of items in the clean set were mislabelled as malware, thus denying *Dr.Web* a VB100 award this time.

ESET Security 3.0.3

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	0

The *ESET* installation process returned to the .deb package method, and proved fast and efficient. On-access scanning could be implemented using either *dazuko* or the *Samba* VFS path, and the latter was adopted at the request of the developers. This proved simple to get working once I had navigated my way



File access lag time	Archive Files				Binaries and System Files				Linux Files				Media and Documents				Other File Types			
	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!	972	0.26	973	0.26	554	0.13	555	0.13	856	0.19	857	0.19	158	0.06	159	0.06	143	0.10	144	0.10
AVG Anti-Virus	76	0.02	1791	0.48	534	0.13	814	0.20	2848	1.27	3465	1.60	358	0.17	398	0.19	362	0.34	476	0.46
Avira AntiVir	68	0.02	835	0.22	354	0.08	491	0.12	2506	1.08	2598	1.13	330	0.16	339	0.16	356	0.33	356	0.33
BitDefender Security	1700	0.46	1700	0.46	780	0.20	780	0.20	2865	1.27	2865	1.27	364	0.17	364	0.17	389	0.37	389	0.37
Doctor Web Dr.Web	2726	0.74	2726	0.74	980	0.25	980	0.25	2507	1.08	2507	1.08	342	0.16	342	0.16	359	0.33	359	0.33
ESET Security	2367	0.64	2367	0.64	1618	0.42	1618	0.42	1611	0.60	1611	0.60	208	0.09	208	0.09	152	0.11	152	0.11
Frisk F-PROT	386	0.10	386	0.10	677	0.17	678	0.17	1054	0.29	1055	0.29	150	0.06	151	0.06	150	0.11	151	0.11
F-Secure Linux Security	137	0.03	4342	1.17	735	0.18	1030	0.26	2337	0.99	2966	1.33	294	0.14	377	0.18	329	0.30	401	0.38
Kaspersky Anti-Virus	2564	0.69	2564	0.69	753	0.19	753	0.19	2070	0.84	2070	0.84	239	0.10	239	0.10	260	0.23	260	0.23
MicroWorld eScan	3376	0.91	3376	0.91	1141	0.29	1141	0.29	4477	2.15	4477	2.15	484	0.24	484	0.24	471	0.45	471	0.45
Norman Virus Control	102	0.03	NA	NA	652	0.16	NA	NA	1850	0.72	NA	NA	190	0.08	NA	NA	250	0.22	NA	NA
Quick Heal	35	0.01	NA	NA	240	0.05	NA	NA	1686	0.64	NA	NA	200	0.08	NA	NA	187	0.15	NA	NA
Sophos Anti-Virus	121	0.03	1173	0.32	581	0.14	645	0.16	1573	0.57	1699	0.64	227	0.10	230	0.10	251	0.22	257	0.22
Symantec AntiVirus	353	0.09	NA	NA	465	0.11	NA	NA	1713	0.65	NA	NA	221	0.10	NA	NA	243	0.21	NA	NA
VirusBuster SambaShield	73	0.02	NA	NA	591	0.14	NA	NA	1692	0.64	NA	NA	224	0.10	NA	NA	225	0.19	NA	NA

around the setup, and again the command-line scanner was a joy to operate.

Scanning speeds were not as eye-watering as usual, but they seemed much quicker on the infected sets, suggesting that the clean items were being subjected to some thorough probing. With excellent detection and no false positive issues, *ESET* storms its way to a record 50th VB100 award.

Frisk F-PROT Antivirus 6.2.1.4252

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	1

Installation of *F-PROT* took the simple method of extracting an archive onto the system and poking around inside it for the required tools and daemons. Man pages and other hints were plentiful and clear, and setup was a painless process, as was testing itself.

Having become accustomed to the dragged-out nature of the tests so far, *F-PROT*'s scanning speeds seemed lightning-quick, with detection rates equally remarkable. But, just as everything was looking rosy for *F-PROT*, a single item in the clean set – a rather specialist text editing tool – was labelled as a backdoor program, and *F-PROT* therefore fails to make the VB100 grade by a whisker.

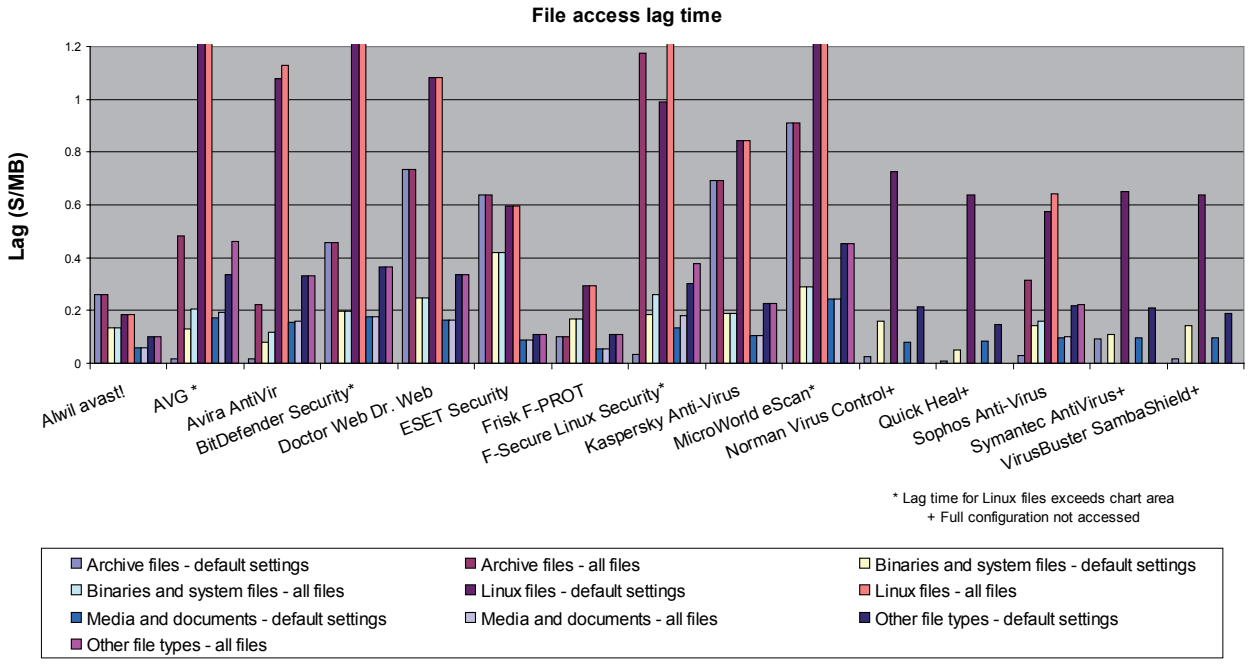
F-Secure Linux Security 7.00.71615

ItW	100.00%	**Polymorphic**	99.88%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	1

F-Secure's product is a lot bigger and shinier, with a complex installation process involving first setting up several dependencies, running the initial installer then running a secondary configuration program. Part of the reason for this bulkiness is the complexity of the product – in addition to the simple anti-virus scanner provided by most submissions this month, *F-Secure*'s product includes its own firewall and a series of intrusion-prevention and integrity-checking tools.

Getting things running was initially a little tricky, requiring in-depth perusal of a lengthy PDF manual included inside the install packages – of course, with no desktop environment on the test systems, this required copying it back to the client machine (and installing PDF viewing software) to read it. On first attempt the product claimed its on-access component was active, but it seemed to be having no effect, and the web interface – which appeared to be the only means of accessing much of the configuration – was inaccessible beyond the login page.

On second attempt things went much better, however – the on-access scanner, apparently based on a custom version of the *dazuko* technology, worked fine and the



web interface presented a pleasant and well-laid-out experience.

I operated on-demand scanning via the command line as usual, and other tests also proceeded normally after a few tweaks to the settings via the GUI. Scanning speeds were fairly languid once again, but scanning levels were thorough and detection equally in-depth. Just when all was looking up, the same tool that tripped up *F-PROT* was alerted on, this time being labelled an Ircbot trojan. This meant that *F-Secure* was also denied a VB100 award this month, and as the alert was marked as originating from the *AVP* engine, more upsets were expected.

Kaspersky Anti-Virus for Samba Servers for Linux 5.5

ItW	100.00%	**Polymorphic**	99.88%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	1

Kaspersky uses the .deb package method for its install, but this time it seemed to do little more than place the required software in the right spots; exactly where these spots might be was left somewhat unclear. After some rummaging around I found the manual pages and linked them in with the man system, which shed some light on how to proceed. Post-install scripts had doctored my *Samba* configuration to include the VFS on-access scanner, which was fairly simple to configure. The command-line scanner operated in a fairly normal way too, although it had an unwieldy title and required to be run as root to access its own configuration files.

Once things were up and running everything went fairly smoothly, with speeds not too bad in a slow month like this. Detection rates were excellent as ever, including complete coverage of the WildList, but as expected that pesky false positive cropped up once more and K*aspersky Lab* fails to add another VB100 award to its collection.

MicroWorld eScan for Linux Server 2,0-16

ItW	100.00%	**Polymorphic**	99.88%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	1

After the performance of the last few products, things did not bode well for *MicroWorld*, which is another product based on *Kaspersky*'s *AVP* engine.

The installation process was another complicated monster, with an enormous list of dependencies thoughtfully provided by the developers. While much of the list could be acquired from repositories on the platform's install CD, many more items had to be scavenged from the Internet. Many of them seemed to relate to the graphics display,

Archive scanning depth		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
Alwil avast!	OD	X	X	√	X	X	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√
AVG Anti-Virus	OD	X	√	√	X	√	X	√	√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avira AntiVir	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Security	OD	√	√	√	√	√	8	√	8	√
	OA	√	√	√	√	√	8	√	8	√
Doctor Web Dr.Web	OD	X	√	√	√	√	√	√	√	√
	OA	X	7	7	7	7	3	7	3	√
ESET Security	OD	√	√	√	√	√	5	√	√	√
	OA	√	√	√	√	√	5	√	√	√
Frisk F-PROT	OD	1	5	5	√	5	2	5	5	√
	OA	1	5	5	X	5	2	5	5	√
F-Secure Linux Security	OD	√	6	6	6	6	3	6	6	√
	OA	X/√	X/6	X/6	X/6	X/6	X/3	X/6	X/6	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
MWTI eScan	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Virus Control*	OD	X	X	√	√	X	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
Quick Heal*	OD	2	√	√	X	√	1	√	X	√
	OA	2	X	X	X	X	X	X	X	√
Sophos Anti-Virus	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Anti-Virus*	OD	X	X	3	3	3	3	3	3	√
	OA	X	X	3	3	3	3	3	3	√
VirusBuster*	OD	2	√	X	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√

Key:

X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

[1-9] - Archives scanned to limited depth

X/√ - Default settings/thorough settings

*Increased archive handling options not accessed in some products

so I assumed they were required to support some kind of interface, which would not be required. Aided by detailed instructions provided by the developers I gathered them up and eventually managed to get all the *eScan* components, most of which were provided as .deb packages, to install and run.

Once everything was happy, and after another tweak to a *Samba* configuration file to activate a VFS object, the test chugged along at a fairly laid-back pace, the default settings being extremely thorough. In the end things went much as predicted, with excellent detection rates throughout and just that single pesky little file mislabelled in the clean set spoiling *MicroWorld*'s hopes for a VB100 award.

Norman Virus Control 5.701

ItW	100.00%	**Polymorphic**	73.47%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	99.00%
File infectors	99.15%	**False positives**	0

With *Norman* we returned once more to the simple and trusty method of dropping an archive load of files into the filesystem root. This did a splendid job, setting everything up just so, including the man pages, which enabled fast and easy navigation of the configuration process. With the *dazuko* module loaded once again, everything looked set to go in record time.

Getting through the on-demand tests proved a breeze, thanks to the lucid instructions and logical controls. The on-access monitoring seemed solid and functional, although slightly lower in detection of some file-infecting viruses thanks to the *Sandbox* technology playing less of a role by default. Looking to change these settings, all the advice I could find referred me to a Java-based interface, but getting access to this would require considerable effort and time – which was running short.

Skipping the added speed measurements with full scanning enabled, a quick look through the logging showed that *Norman* had brought a run of recent misses to an end with excellent WildList detection and no false positives, bringing it proudly back to VB100 certified status.

Quick Heal 9.50

ItW	100.00%	**Polymorphic**	83.86%
ItW (o/a)	100.00%	**Linux**	66.67%
Worms & bots	99.87%	**Legacy**	93.95%
File infectors	98.43%	**False positives**	2

Quick Heal is another *dazuko* product, which also had a few other dependencies to fill. This proved to be a fairly straightforward job thanks to some tips from the developers.

The setup process was clear, helpful and even colourful, making a surprising and impressive difference to the clarity of an installation, which can often get swamped in a mass of samey text. Getting to grips with the command-line scanner proved a little less smooth, with a rather unusual syntax required including putting the path to files to be scanned before all other arguments. A GUI is also available, for those hedonists running glitzy desktop environments, but the command line served ably once its intricacies had been mastered.

The product lived up to its name with its scanning speeds, which were helped in the on-access test by not scanning archives by default. Upon investigating this, I found various options for the configuration of on-access logs and other sundries, but little concerning the actual types of files scanned. Of course, I may have been looking in the wrong place. Moving swiftly on to the results, I found detection rates at their usual decent level with excellent scores on the WildList and other more recent samples, but once more a couple of items in the clean set were alerted on and *Quick Heal* misses out on a VB100 award this month.

Sophos Anti-Virus for Linux 6.3.3

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	65.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	0

Sophos's product is unusual in this test in using its own file-hooking setup. This goes by the name of *Talpa* and apparently, like *dazuko*, has been made open-source but is not as widely implemented. This gave rise to a few worries, as the platform under test is rather new and as yet not officially supported. However, after some confusion over which version I should be using, things went like a dream.

The product is supplied as a simple .tgz archive and an installation script which prepares and sets up everything very neatly, including pleasantly accessible documentation.

The command-line scanner uses pretty straightforward and humanly readable syntax, and scanning times were excellent with the bare, no-options settings. Tweaking them up a bit still produced good speed, and the on-access scanner was similarly zippy, although working out the rather less straightforward configuration system took a few moments. In the end, detection rates were top-notch, false positives absent, and *Sophos* put some upsets in recent tests behind it by winning a VB100 award with ease.

Symantec AntiVirus 1.0.4.516

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Linux**	100.00%
Worms & bots	100.00%	**Legacy**	100.00%
File infectors	100.00%	**False positives**	0

I approached *Symantec*'s product with some dread, remembering a rather traumatic experience with its Byzantine configuration system in last year's *Linux* test. Searching inside the pair of archives provided I found a selection of .deb packages and some documentation in PDF files, which were shipped over to the workstation for some in-depth browsing. Eventually, after a few false starts thanks to conflicting instructions at different points, things were up and running pretty solidly.

Next came the equally arduous task of navigating my way around the product, which was carried out mostly by means of passing arguments to the 'sav' command, which would then silently be followed by the scanning and monitoring daemons. This made monitoring the progress of scans rather tricky, having to rely mainly on watching the tail of the syslog – the only logging method available as far as I could tell – and keeping an eye on the hard drive activity lights.

On-access monitoring defaults to removing or disinfecting files, so to speed things along I delved bravely into the full glory of the configuration system, digging up secrets gleaned from tech support gurus for the last test. A listing of the configuration settings, which take the form of a registry-style database of keys, provided a little illumination, but its true meanings were far from clear. Passing in commands proved a lengthy and difficult process. Building up huge commands to pass in simple changes and

an absence of feedback to confirm an instruction had been accepted, required repeated trawls through the data to check changes had indeed occurred.

Once everything was under control, things moved along nicely, with excellent scanning speeds and the usual impeccable detection. Archive settings were a little low to measure fairly against others on the speed graphs, but changing them would have required more visits to the config system, and the resultant wear and tear on keyboards would have eaten heavily into my hardware budget. Leaving things as they were, *Symantec*'s perfect detection scores across all test sets and absence of false positives earns it yet another VB100 award.

VirusBuster SambaShield 1.2.0_10

ItW	100.0%	**Polymorphic**	79.29%
ItW (o/a)	100.00%	**Linux**	83.33%
Worms & bots	99.91%	**Legacy**	99.92%
File infectors	99.21%	**False positives**	0

The final product on the list came from *VirusBuster* and proved a much more pleasant experience. Provided as a pair of archives with perl installation scripts, the setup ran through speedily and without difficulty. Another *Samba* VFS object managed the on-access side of things, and the layout and syntax seemed generally well thought out and sensible.

The tests zoomed through at an impressive rate, and detection levels showed continued improvement. Again a lack of time prevented in-depth investigation of the on-access configuration system to enable full archive scanning, but the only other problem encountered was the layout of the logging, keeping the scanned path on a separate line from detection information, which entailed a few extra stages to my results parsing. Beyond this minor quibble, though, the WildList was covered without problems, and the rest of the sets handled pretty well too, and without any false positives either *VirusBuster* earns a VB100 award.

CONCLUSIONS

Once more the *Linux* test has proved to be the domain of the hardened VB100 experts, the small list of products participating in this test consisting entirely of names made familiar from consistent and dogged appearances in the test month after month. A few regulars were notable by their absence, with some of the larger, more corporate-focused companies yet to implement support for the platform selected.

After a string of low-scoring tests I had hoped that this month might finally see a clean sweep with all products passing, and as far as the WildList went we nearly made it, with only one product having trouble in this area. Once again, however, the test's strict false positive rules played a major part, with just four files scuppering the chances of a VB100 award for six of the products.

Beyond the basics of the scores, the products themselves displayed a dizzying variation in style and implementation, with some remaining extremely simple while others have expanded their functionality in a range of new ways. Both paths proved capable of providing stable, rapid and usable products as well as confusing, sluggish and wobbly protection, with documentation – or at least accessing it – being the most significant factor as far as ease of use was concerned. Of course, submissions were not necessarily made in the same format as paying customers would receive, and the likelihood of more obvious installation instructions and user manuals would make a big difference in some cases. With a little work, however, all products were made to function sufficiently well to get through the tests, and all provided a decent level of configurability, albeit in some cases in a rather bizarre and arcane fashion.

The added complexity of the installation and navigation of various products meant that this month's comparative was not the quick and restful experience I had hoped for between two much larger tests. It has highlighted the pace with which most products are keeping up with our test sets, and the need for more rapid expansion of those test collections to provide a more accurate gauge of their capabilities. Hopefully, June will grant time to ensure the test sets are well enlarged in time for the forthcoming *XP* comparative, due to commence at the start of July and to appear in the August issue of *VB*. Perhaps that test, which I expect to break the 40 product mark, will finally see that clean sweep with no failures – I can but hope.

Technical details:

Tests were run on identical machines with *AMD Athlon64* 3800+ dual core processors, 1 GB RAM, 40 GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, running *Ubuntu Linux 8.04LTS Server* edition.

Client machines had 1.6 GHz *Intel Pentium* processors with 512 MB RAM, 20 GB dual hard disks, CD-ROM and 3.5-inch floppy drive running *Microsoft Windows XP Professional SP2*, connected via *Samba 3.0.28a*.