COMPARATIVE REVIEW

RED HAT LINUX 9

Matt Ham

With *Linux* still making gradual headway in the operating system battleground it comes as little surprise that there are more products in this year's *Linux* comparative than the last, or that the products submitted this year are more feature-packed. On the last occasion 14 products were submitted; this time there are 17.

The additions to the line up for this test are: *Avira*, *MicroWorld*'s *eScan* and *Norman Virus Control*. All of these are from companies that are familiar with *VB*'s testing regime – indeed, *Avira* is developed by the same team that produces *H+BEDV*'s *Antivir*, so they have first-hand experience of testing on the *Linux* platform too.

In the last *Linux* test there were problems of a technical nature and problems that were more informational in nature. Technically, the on-access scanners were a very mixed bag, ranging from stable to likely to fall over at the drop of a pin. In last year's test neither the *Sophos* product nor the *McAfee* product had an on-access scanner. *McAfee* has since added this functionality, leaving *Sophos* as the odd man out in this year's review.

The majority of *Linux* products use *Dazuko* as their on-access scanning solution, which proved to be reliable last year. Twelve months on, even greater stability should be expected all round.

The second problem encountered in last year's *Linux* review related to updating the products, it not always being apparent how updates should be applied without direct access to the Internet. This is an increasing problem on all platforms since Internet access is considered to be a standard feature these days. Such reasoning can render it very difficult to update an isolated machine before connecting it to the net – clearly protection is required *before* connecting a machine to a resource that is plagued with a multitude of threats ready to attack a vulnerable machine. It seems quite common for developers to ignore this issue, however, so I was prepared for updating to be a major problem.

The other complaint arising from last year's *Linux* comparative concerned product documentation. Although still not ideal, the documentation seemed less problematic this time.

TEST SETS

The test sets were updated to the latest WildList data available on 24 February 2005. In fact, this was the December 2004 data. The deadline for product submissions was 28 February 2005, meaning that the task ahead of the products was somewhat less than taxing, since their developers had each had a full two months to react to files submitted by customers or obtained from other developers. Additions to the WildList this time consisted of a further bunch of tedious worms and, again, these were not expected to present any significant challenge for the products.

Alwil Avast 1.0.8.2

ItW File	100.00%	**Macro**	99.56%
ItW File (o/a)	100.00%	**Standard**	99.36%
Linux	50.00%	**Polymorphic**	93.57%

Avast is a *Dazuko*-based scanner as far as on-access functionality goes, and has moved from late beta to a fully released product over the last year. On this occasion the only major sticking point was the application of a licence file to the product which was not named as the product expected (due to *Linux* case-sensitivity), causing the *Avast* daemon to refuse to operate. Once this problem had been overcome, however, all was plain sailing. As far as installation was concerned *Avast* differed slightly from the majority of other products, in that it spread its files far and wide. Most installations in this test were located in the opt directory, which seems to be a *de facto* standard.

Problems encountered with *Avast*'s on-access scanner in previous reviews had vanished and detection rates were very similar to those obtained last year, so it is no surprise that *Alwil* receives another VB 100% award in this test.

Avira Avira 1.1.3-17

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	91.67%	**Polymorphic**	100.00%

As mentioned earlier, *Avira* is a 'new' product that does not really count as such, since its developer, *H+BEDV*, is an old hand at *VB* comparative testing and also very much connected with the *Dazuko* project. It comes as little surprise, therefore, that the on-access scanner is powered by this module. Installation of the product was easy and its detection was excellent – better even than the *Windows* product reviewed earlier this year (see *VB*, February 2005, p.12). The detection rate does come at a price though: this is one of the noticeably slower scanners in the line-up. There were no false positives to mar the performance and thus *Avira* receives a VB 100% award.

On-access tests	ItW file		Macro		Polymorphic		Standard		Linux	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast	0	100.00%	18	99.56%	114	93.44%	14	99.54%	9	80.00%
Avira Avira	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	86.67%
CAT Quick Heal	0	100.00%	74	98.20%	314	96.25%	103	96.35%	7	60.00%
Doctor Web Dr.Web	0	100.00%	0	100.00%	0	100.00%	2	99.82%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	93.33%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	0	100.00%	2	99.72%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	425	83.72%	42	97.33%	16	48.33%
H+BEDV Antivir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	86.67%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	93.33%
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	1	99.91%	0	100.00%
Norman Virus Control	0	100.00%	10	99.75%	147	92.09%	10	99.57%	6	66.67%
SoftWIN BitDefender	0	100.00%	26	99.31%	6	99.73%	21	99.42%	8	73.33%
Sophos SWEEP	-	-	-	-	-	-	-	-	-	-
Trend Micro ServerProtect	0	100.00%	0	100.00%	215	95.77%	10	99.53%	7	65.33%
VirusBuster VirusBuster	3	99.76%	3	99.93%	3048	77.13%	68	97.12%	37	26.67%

CAT Quick Heal X Gen 7.03

ItW File	100.00%	**Macro**	98.20%
ItW File (o/a)	100.00%	**Standard**	96.33%
Linux	60.00%	**Polymorphic**	96.25%

In last year's review only one product offered a GUI, so it came as something of a surprise to note that an increasing number of products in this test had GUI functionality. *CAT*'s product was the first of these. *CAT*'s GUI is QT-based and totally optional, and was not, therefore, used for scanning purposes. This was the default decision taken wherever a GUI could easily be avoided, since the majority of products are significantly easier to test from the command line.

That said, the results for ItW scanning were perfect, with just a few misses in the other test sets. The speed of scanning was also towards the faster end of the spectrum. *Quick Heal* gained a VB 100% on its first test on *Linux* last year, and easily obtains another on this outing.

Doctor Web Dr.Web for Linux 4.32.2

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	100.00%

Dr.Web is the first product in this review which does not use *Dazuko* for on-access scanning. Instead, it uses a vfs object called by the Samba daemon. Historically these solutions have been slightly prone to hiccups, although *Dr.Web* seems to have avoided these consistently. No problems of any type were noted during installation or operation, and all but two files on access were detected in the whole of the test sets. *Dr.Web* thus continues its good work and gains another VB 100% as a result.

Eset NOD32 2.03

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	100.00%

Having dabbled with kernel objects in the past, the *Eset* developers have now opted for the simpler life and use *Dazuko* for on-access scanning. The last test of this product on *Linux* demonstrated no technical problems but a whole host of different operations were required to install and configure the product. This has been simplified significantly, with one RPM file replacing the trickery that was required previously. The results of scanning were eminently predictable: all files were detected, with a VB 100% award the equally predictable result.

F-Secure Anti-Virus 4.62

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	93.33%	**Polymorphic**	100.00%

F-Secure Anti-Virus (*FSAV*) proved to be a very frustrating beast initially, with all attempts to tame it failing dismally. However, this changed instantly when it became apparent that there are two copies of the configuration file for the product. Altering one set seems to have no effect whatsoever, and was the cause of the initial frustration. Once the operational files had been edited appropriately, no problems were encountered as the tests proceeded. A VB 100% therefore wings its way to Finland.

Of note with this product were the relative sizes of the product and definition files. The full product totalled 6.9 MB, a little above the average for the *Linux* products reviewed here. The additional definition files, however, were 7.1 MB in size – larger than the product itself.

FRISK F-Prot Antivirus 3.16.6

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	99.82%
Linux	100.00%	**Polymorphic**	100.00%

Last year *FRISK*'s product was notable for its slow speed of scanning. However, this problem seems to have been banished in the intervening months.

No longer as closely related to *FSAV* as it once was, the two products are beginning to show a divergence in their test results. Not a major divergence though, since *FRISK* missed only one sample across the whole test set (which was not in the wild) and duly qualifies for a VB 100% award.

Grisoft AVG 7 Anti-Virus 7.0.15

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	97.15%
Linux	41.67%	**Polymorphic**	83.72%

AVG is yet another *Dazuko*-based scanner, although unlike most other *Dazuko*-based products it does not set up shares to be scanned automatically – these must be designated manually. Even with this requirement, however, less tweaking was required this time than was necessary last year, for which my thanks go to *Grisoft*.

Files missed during scanning were very much the same as those usually missed by *AVG* – the weakness of the scanner lying in complex polymorphic viruses. Since real viruses are almost never seen these days, however, this is not the issue that it once appeared likely to be. With perfect detection of samples in the wild, *AVG* is worthy of a VB 100% award.

H+BEDV Antivir 2.1.3-17

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	91.67%	**Polymorphic**	100.00%

Despite ostensibly being the same product as *Avira*, the *Antivir* package weighs in at well over twice the size of its relative (a sturdy 8.8 MB in comparison with *Avira*'s 3.4 MB). The reason for this soon became apparent, however, since a Java-based GUI is included in the package.

On-demand tests	ItW file		Macro		Polymorphic		Standard		Linux	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast	0	100.00%	18	99.56%	113	93.57%	15	99.36%	14	50.00%
Avira Avira	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	91.67%
CAT Quick Heal	0	100.00%	74	98.20%	314	96.25%	104	96.33%	7	60.00%
Doctor Web Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	93.33%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	0	100.00%	1	99.82%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	425	83.72%	44	97.15%	17	41.67%
H+BEDV Antivir	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	91.67%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
MicroWorld eScan	177	58.67%	0	100.00%	0	100.00%	20	97.71%	7	60.00%
McAfee LinuxShield	0	100.00%	0	100.00%	0	100.00%	2	99.82%	0	100.00%
Norman Virus Control	0	100.00%	6	99.85%	147	92.09%	6	99.66%	1	93.33%
SoftWIN BitDefender	0	100.00%	33	99.14%	6	99.73%	22	99.23%	11	53.33%
Sophos SWEEP	0	100.00%	8	99.80%	0	100.00%	15	99.30%	8	58.33%
Trend Micro ServerProtect	0	100.00%	0	100.00%	182	96.22%	8	99.66%	4	93.33%
VirusBuster VirusBuster	3	99.76%	0	100.00%	3074	77.01%	66	97.24%	29	53.33%

This was not tested. Other than this difference, *Antivir* and *Avira* were identical. Command line options and detection were the same for both products, with timing tests the same within the tolerances of such tests.

It should not take great detective skills, therefore, to realise that *Antivir* also receives a VB 100%.

Kaspersky Anti-Virus 5.0.3.0 build 15

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	100.00%
Linux	100.00%	**Polymorphic**	100.00%

There was a problem with *KAV* concerning the installation of additional virus databases. However, I was forewarned of this by the product developers, and so I was spared some frustration.

In last year's comparative tests the product's documentation and installation in general proved problematic, but there were no issues with these on this occasion, which was something of a relief.

Operating as a vfs object, the Samba scanning operated perfectly, blocking all infected objects. The on-demand scanner equalled this detection, with a VB 100% for *Kaspersky* as the result.

MicroWorld eScan Antivirus 1.0A

ItW File	58.67%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	97.71%
Linux	60.00%	**Polymorphic**	100.00%

A new addition to the *Linux* comparative, *eScan* proved to be a mixed bag of problems and delights. Of all the products supplied using *Dazuko*, *eScan* is the only one that includes the *Dazuko* source and that configures and makes *Dazuko* automatically during installation. After this pleasant surprise the GUI was launched, which is the interface for on-access scanning, and it was here that matters became a little confusing, since the GUI offers no obvious way in which to perform on-demand scans.

After updating the product the GUI indicated new definition dates and thus testing was commenced. The results were very good indeed on access. On demand was another matter however – a whole host of files were missed. These were a mixture of older and newer files, though most were newer. Assuming this to be a definitions issue the updates were checked again, but all seemed to be in order.

Another oddity was encountered upon invoking the on-demand scanner on a directory with no leading or trailing '/' supplied. Here, a segmentation fault was triggered. With these problems on demand it comes as no surprise that a VB 100% cannot be awarded to *eScan* on this occasion.

McAfee LinuxShield 1.1.0.665.i686

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	99.82%
Linux	100.00%	**Polymorphic**	100.00%

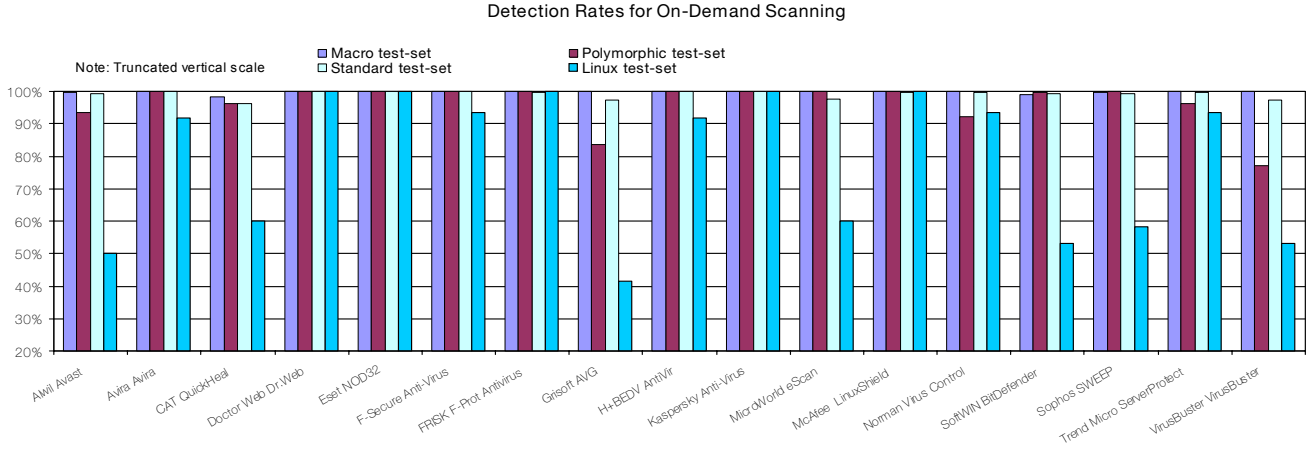
LinuxShield is the new name for *McAfee*'s *Linux* offering. In this case a GUI is mandatory. The only way to perform on-demand scans conveniently is through the GUI. Performing them from the command line requires scan parameters to be set up via the GUI – so in this case the GUI was used for on-demand testing. Updating seemed a little awkward from a local directory, in that engine updates worked, while definition updates did not. These were performed by copying the definitions manually to the correct area.

The only false positive of the tests occurred with *LinuxShield*, though this was not a serious one – the file being flagged as a 'program' rather than as a real virus. Since the file in question was a reboot utility, this flag seemed justified. Scanning was good as far as detection was concerned, so this new incarnation gains a VB 100% where its predecessor failed.

Norman Virus Control 5.70.01

ItW File	100.00%	**Macro**	99.85%
ItW File (o/a)	100.00%	**Standard**	99.66%
Linux	93.33%	**Polymorphic**	92.09%

The on-access functionality in *Norman Virus Control* (*NVC*) is new – in fact, it is so new that some documentation states that it does not yet exist. The on-access scanner uses *Dazuko* to scan and performed well. However, it seems that it can be configured only via the Java-based GUI. On-demand scanning, meanwhile, is perfectly configurable through the command line. In the end, results for *NVC* were much the same as have been seen in recent comparatives on other platforms and *NVC* is awarded a VB 100%.



Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files		Linux Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time (s)	Throughput (kB/s)	Time (s)	Throughput (kB/s)
Alwil Avast	138	3963.3		12.1	6556.5		23	6931.2	6.1	12230.7	6.0	4503.4
Avira Avira	416	1314.7		7.2	11018.6		193	826.0	12.4	6016.7	4.3	6283.9
CAT Quick Heal	64	8545.8		13.0	6102.6		45	3542.6	17.3	4312.6	4.4	6141.0
Doctor Web Dr.Web	186	2940.5		11.6	6839.1		85	1875.5	15.3	4876.3	5.4	5003.8
Eset NOD32	40	13673.3		4.5	17629.7		19	8390.3	1.5	49738.3	2.2	12282.1
F-Secure Anti-Virus	168	3255.5		15.9	4989.5		86	1853.7	32.7	2281.6	8.0	3377.6
FRISK F-Prot Antivirus	114	4797.7		4.8	16527.9		50	3188.3	5.3	14076.9	2.0	13510.3
Grisoft AVG	99	5524.6		11.2	7083.4		74	2154.3	13.4	5567.7	16.3	1657.7
H+BEDV Antivir	358	1527.7		7.7	10303.1		201	793.1	11.0	6782.5	4.9	5514.4
Kaspersky Anti-Virus	143	3824.7		15.1	5253.9		62	2571.2	16.9	4414.6	8.3	3255.5
MicroWorld eScan	66	8286.9		16.1	4927.6		80	1992.7	46.2	1614.9	8.0	3377.6
McAfee LinuxShield	170	3217.2	[1]	12.0	6611.1		79	2017.9	17.0	4388.7	7.0	3860.1
Norman Virus Control	523	1045.8		8.1	9794.3		481	331.4	8.2	9098.5	1.7	15894.4
SoftWIN BitDefender	304	1799.1		7.5	10577.8		165	966.2	7.9	9444.0	15.9	1699.4
Sophos SWEEP	64	8545.8		11.4	6959.1		45	3542.6	12.7	5874.6	5.9	4579.8
Trend Micro ServerProtect	88	6215.1		5.0	15866.8		29	5497.1	7.0	10658.2	4.0	6755.1
VirusBuster VirusBuster	137	3992.2		9.7	8178.7		83	1920.7	15.0	4973.8	6.7	4032.9

SoftWIN BitDefender 1.6.2-0

ItW File	100.00%	**Macro**	99.14%
ItW File (o/a)	100.00%	**Standard**	99.23%
Linux	53.33%	**Polymorphic**	99.73%

BitDefender's performance in the last comparative review was marred both by unexpected missed files and by a tendency for the Samba share to lose connections. Happily, both of these problems have been fixed in this latest version.

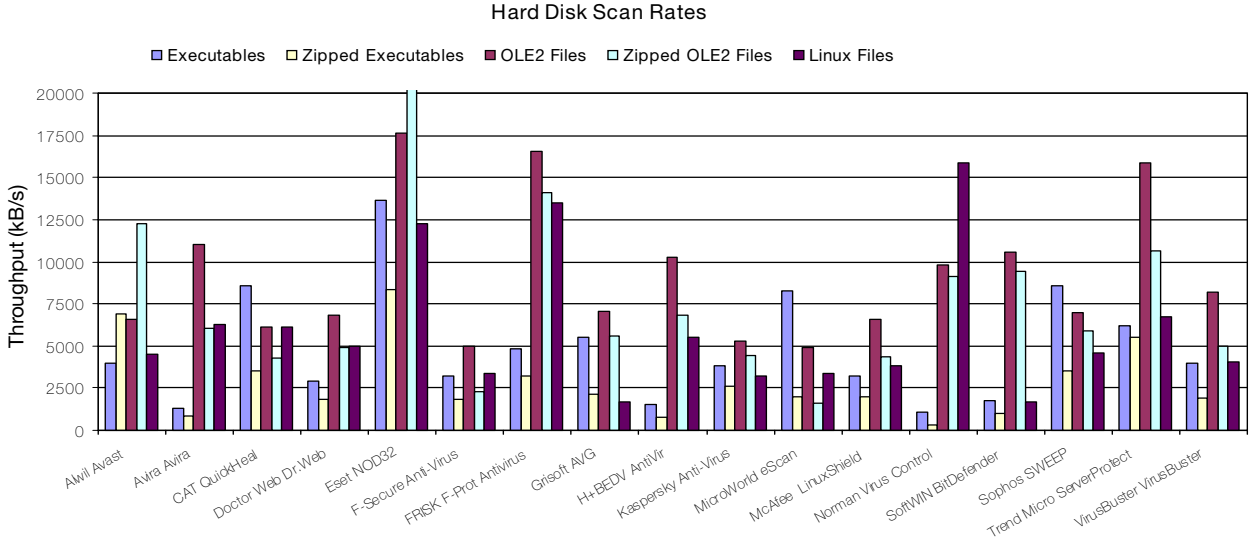
The only slight surprise for *BitDefender* was the fact that the product missed more files on demand than on access. Detection results were generally good, however, and no files were missed in the all-important ItW test set. These improvements are sufficient to justify the award of a VB 100% for this test.

Sophos SWEEP 3.91.0

ItW File	100.00%	**Macro**	99.80%
ItW File (o/a)	N/A	**Standard**	99.30%
Linux	58.33%	**Polymorphic**	100.00%

As mentioned already, *Sophos*'s *SWEEP* is the only product in this comparative review which exists purely as an on-demand scanner. Its lack of an on-access scanner discounts it instantly from a VB 100% award.

Other than this, results for on-demand scanning were good, although detection rates were slightly low in the *Linux* test set. However, the misses in this set are indicative of a general issue with some of the *Linux* worms in the test set. Some of these, such as Linux/Lion, are packaged as archives in their transmitted state. Along with several other products, *SWEEP* does not detect inside archives in its default state.



Trend Micro ServerProtect 2.452.00 7.510

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Standard**	99.66%
Linux	93.33%	**Polymorphic**	96.22%

ServerProtect was among the first products to operate within a GUI and continues to do so – with scanning outside the GUI not easy. For this reason tests were performed from within the GUI. Polymorphic samples represented the bulk of misses for *Trend*'s product, with there being a noticeable increase in the number of misses when scanning on access. These notwithstanding, results were ample for a VB 100% to be awarded. A slight worry was the continuation of a bug that was noted in the product a year ago. When accessing the http-based GUI one URL is slightly garbled. This occurs in exactly the same way today as it did 12 months ago.

VirusBuster VirusBuster 2005 1.1.1

ItW File	99.76%	**Macro**	100.00%
ItW File (o/a)	99.76%	**Standard**	97.24%
Linux	53.33%	**Polymorphic**	77.01%

VirusBuster's scanner showed some strange patterns in detection and as a result tests were performed in several fashions. During the course of these it became apparent that files can neither be either deleted nor quarantined if they contain infected objects such as *PowerPoint* objects. However, the main reason for the additional scans was the fact that samples of W32/Bugbear.B were missed both on access and on demand. Since these are in the wild, this was enough to deny *VirusBuster* a VB 100% award.

CONCLUSION

As was hoped at the outset of this review, the stability of the scanners in this test has shown significant improvement since last year and, in many cases, the installation procedures have become substantially simpler.

However, there were still some issues with updating products and some products are still far less than intuitive to set up. The arrival of more GUIs on the scene is something of a mixed blessing. On the one hand the use of a GUI can be easier for configuration – but on the other, a *Linux* application without full command-line control seems inherently wrong. Although I foresee that the scanners will become increasingly similar to *Windows* applications as far as GUI-centric operation is concerned, it would be appreciated if this were also extended to general ease of use.

Technical details

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive running Red Hat Linux 9, kernel build 2.4.20-8 and Samba version 2.2.7a. An additional machine running Windows NT 4 SP 6 was used to perform read operations on the Samba shared files during on-access testing.

Virus test sets: Complete listings of the test sets used can be found at http://www.virusbtn.com/Comparatives/Linux/2005/test_sets.html. A complete description of the results calculation protocol can be found at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.