COMPARATIVE REVIEW

NOVELL NETWARE 6.5

John Hawes

Last month the annual *VB* conference saw representatives from across the security industry get together to share new ideas and observations, and where necessary criticise them mercilessly. My mind was fizzing with new information and ideas when I returned to the *VB* test lab, but unfortunately that was soon overshadowed by the sound of another, rather less helpful fizzing, along with some alarming pops, bangs and puffs of smoke that indicated a series of cataclysmic hardware failures. The resulting shortage of test systems was compounded by a hardware failure of a more biological nature, which sliced further chunks of time out of what was already a tight schedule.

All this is by way of explanation for those who were expecting to find this comparative review included in the October issue of *Virus Bulletin*, as well as for the fact that some of the detail normally provided is missing from this review. The testing of scanning speeds in non-default modes, usually recorded to afford a more accurate comparison of processing efficiency, was omitted this month, but I hope to reinstate this test in the next review.

Novell NetWare brings me full circle, having been the subject of my first, tentative venture into the battleground of comparative testing (see *VB*, August 2006, p.15). A little over a year has passed, and little seems to have changed in the world of *NetWare* – the platform is still rumoured to be on the brink of demise, yet it still plods along, resolutely refusing to give up the ghost. The purchase of *SuSE* by *Novell* some years back brought hopes of a resurgence for the company and for *NetWare*, but the growing dominance of *Linux* products in *Novell*'s lineup seems to hint at a less glorious future, with *NetWare* functions simply ported to the new platform. The next major release looks likely to include *NetWare* only as a virtual system running on *Linux* hosts.

Whether this is the last VB100 comparative to be run on the platform will depend greatly on the interest shown in this month's review. The number of anti-malware products that continue to support the platform came as something of a surprise to me, as the number of participants actually rose, from last year's scant eight entries to a slightly more bustling 10. This meant I had a couple of new experiences to face, but I hoped that my scrawled notes from the earlier test would help me get around most of the offerings.

PLATFORM AND TEST SETS

NetWare 6.5, nowadays also known as *Novell Open Enterprise Server*, is currently on its sixth service pack. On the surface it bears great similarity to previous editions, and as far as the basics of installing the system are concerned, little seems to have changed. All the old tools continue to be provided, although quite often one can navigate happily to a familiar page to carry out a standard task, only to find that the functionality has been moved elsewhere.

Setting up the DOS boot partition and main system area along with another partition to host the test sets was a very quick process, and the NSS file system seemed as rapid and stable as ever when bombarded with the large amount of data required. The systems were soon up and running and images taken, although unfortunately my preferred imaging software objected rather strongly to the NSS format and I was forced to roll back to an older method. Client systems were equally easy, and I was able simply to grab some *Windows* systems from an earlier test and install the necessary *NetWare* client software on them.

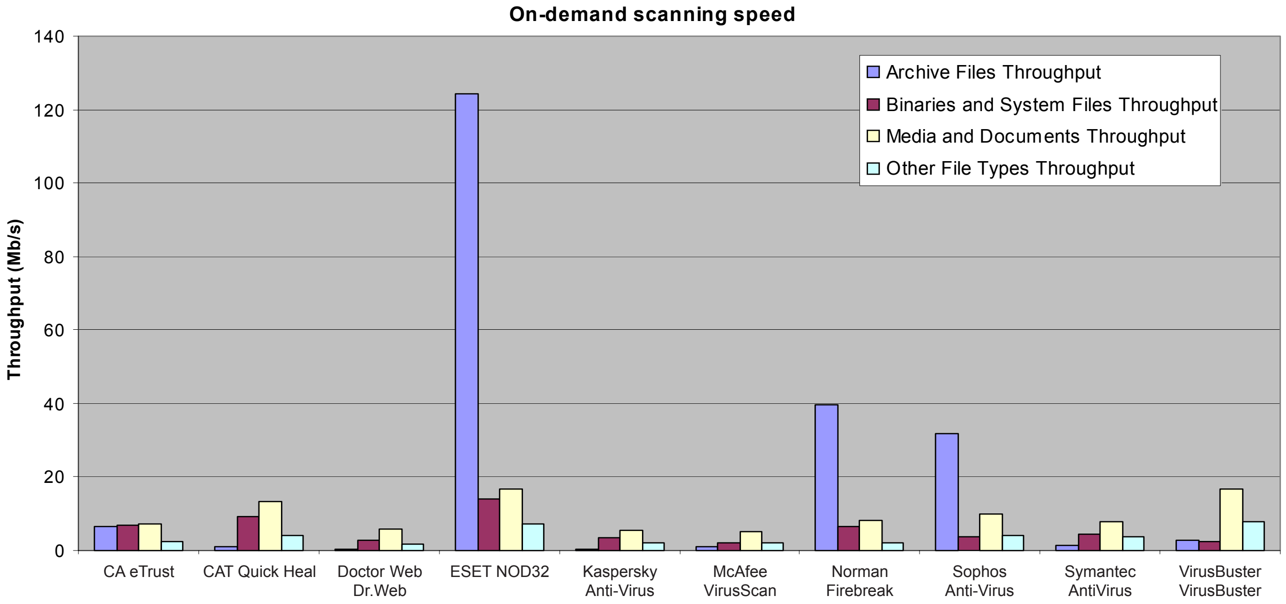
The test sets have undergone some minor enlargements this month. The clean sets saw a handful of new additions, and some of the polymorphic sets which had been deemed a little scantily represented were enlarged appropriately. Updating the WildList set took up the bulk of the available time, with a fairly large number of new arrivals and an even larger number of old items falling off the bottom of the list. Newcomers were mostly modifications of familiar old faces: the W32/Mytobs, Rbots, Sdbots and Strations we have come to expect, plus a few each of the file-infecting W32/Looked and Fujacks, the nasty W32/Rontokbro, and the return of W32/Sircam, which fell off the list some time ago but now claws its way back on.

With the systems and test sets ready, it was time to see if I could remember how all these products worked.

CA eTrust 8.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.67%
File infector	99.86%	**Macro**	99.82%
Polymorphic	99.64%	**False positives**	0

CA's product is part of the *Integrated Threat Management* suite, which presents a pretty standard installer and central management interface across several platforms. I should admit that, as is often the case in these tests, I left this product until towards the end, dreading the epic wrestle that would inevitably be required to beat the system into providing for my needs. Although the central management interface is perhaps perfectly suited to large corporate environments, where squads of highly trained sysadmins skip over its intricacies like graceful mountain



goats, in the setting of the VB100 test lab small and simple usually keeps me happier.

However, on this occasion I was pleasantly surprised. After the installation process via the *Windows* client, with all the standard lengthy EULAs and data-collecting forms, the product fired up on the *NetWare* server showing pages of statistics for files processed and so on. After a small amount of fumbling to find the configuration tool, I discovered a nice simple GUI available on the *NetWare* console, which provided for all my needs and I zipped through the tests without difficulty and without recourse to the ITM remote interface. Even the logs were produced in good old plain text, with none of the bizarrely formatted output of the *Windows* product.

Scanning speeds were good, detection rates across the sets at their usual fairly high level, and with nothing missed in the wild *CA* earns itself another VB100 award.

CAT Quick Heal Antivirus 9

ItW	100.00%	**Worms & bots**	99.83%
ItW (o/a)	100.00%	**DOS**	95.01%
File infector	96.28%	**Macro**	98.24%
Polymorphic	71.63%	**False positives**	0

The *Quick Heal* product came in a much smaller, cosier package – just a couple of NLMs, a zip file and an installer. Running this from the *Windows* client brought up a nice clean-looking install process with no surprises, simply dropping the required files onto the server and making the necessary adjustments to the autoexec.ncf file. However, when I checked back on the server nothing seemed to have started up, so I tried running the NLM files manually, which also seemed to have no effect. A quick and dirty reboot of the server – not ideal for most real-world users – soon got things up and running though.

The product is split into two halves: the real-time scanner module and the on-demand one. The real-time module presents some very basic information about files scanned and how they have been dealt with, along with a list of available options, which proved plenty for my needs. The on-demand part was even simpler, consisting mostly of an empty screen with just the list of options in the middle. It proved simply laid out and easy to navigate, even having a nice ‘browse’ option rather than having to enter paths manually for scanning. The only issue I had with the design was with the choice of actions available on finding a virus, which were limited to delete or repair – neither of which was ideal for my needs.

Running through the tests the product seemed stable and zippy, with some good scanning speeds recorded, but the results showed some oddities which proved repeatable on several retries. The on-demand scores were much as normal for the product, with a fair number of misses across the zoo sets. On-access, however, these misses were amplified considerably, with little clue as to why this should be. Indeed, if the on-access test was run before the on-demand test, the on-demand scanner seemed to become blind to those files passed by the on-access scanners, simply marking them clean.

On-demand tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
CA eTrust	0	100.00%	0	100.00%	235	99.67%	1	99.86%	12	99.82%	9	99.64%		
CAT Quick Heal	0	100.00%	1	99.83%	1057	95.01%	21	96.28%	72	98.24%	1167	71.63%		
Doctor Web Dr.Web	10	98.94%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	9	98.81%	4	3
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.96%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%		4
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Norman Firebreak	0	100.00%	0	100.00%	269	99.12%	10	98.80%	0	100.00%	851	81.55%		
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	10	99.56%	1	
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.54%		1
VirusBuster VirusBuster	0	100.00%	0	100.00%	20	99.77%	11	98.08%	0	100.00%	224	86.17%		

However, none of these issues affected the more recent content in the WildList set, or even the ‘worms and bots’ test set, and since the product did not generate any false positives either, it qualifies for a VB100 award.

Doctor Web Dr. Web for Novell NetWare 4.33.3

ItW	98.94%	**Worms & bots**	100.00%
ItW (o/a)	98.94%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	98.81%	**False positives**	4

Doctor Web’s *NetWare* offering was pretty familiar to me after having tested it last year – it’s a nice simple thing which requires only a few files copying onto the SYS volume of the server and a single NLM loading. This brings up the interface: a stark thing in old-fashioned green-on-white, with not much to it beyond a small menu down one side and a big splash of copyright information filling the rest of the screen.

Once the menu system had been deciphered, the product zoomed through most of the tests in excellent time, although some incredibly in-depth analysis of compressed files on demand made for a pretty lengthy scan over the archive speed set, reporting many more ‘items’ scanned than any other product in this part of the test.

Although time constraints prevented the usual test comparing all products with full archive scanning enabled, *Dr.Web* had sensibly disabled this option on access and got through the test sets in good time, allowing my graphs to show at least some of the picture fairly clearly.

Dr.Web flagged up a handful of false positives in several of the newer areas of the clean sets, mostly with the label ‘Win32.Downloader.trojan’. In the infected sets, scores were pretty good on demand, with only a handful of the new polymorphic additions missed, but on access several file types seemed to be ignored by default, including *PowerPoint* presentations and .HTA files. In the WildList set some six separate items, including two W32/Rbot variants and three W32/Sdbot variants, were all missed, thus extending *Dr.Web*’s run of bad luck in the VB100 tests.

ESET NOD32 2505

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.96%	**False positives**	0

NOD32 on *NetWare* is an even simpler product – again a handful of files dropped into place, providing a command-line scanner and the AMON on-access monitor. All were pretty easy to manage, the default options being generally ideal for my needs (with plenty of clear instructions available for those who want to change them), and the product romped merrily through the tests.

There’s not much else to say about such a pared-down product, beyond the fact that the default for on-demand scanning is, unusually, not to scan inside archive files – a fact which shows itself clearly in the graph of on-demand speeds.

The rest of the speeds were in their normal place at the very top of the rankings in almost all categories, and detection was similarly exemplary, with barely anything missed. With no false positives either, *NOD32* earns yet another VB100 award.

On-access tests	ItW		Worms & bots		DOS		File infector		Macro		Polymorphic		Clean set	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	False positives	Susp.
CA eTrust	0	100.00%	0	100.00%	235	99.67%	3	99.38%	12	99.82%	9	99.64%		
CAT Quick Heal	0	100.00%	1	99.83%	5891	88.39%	32	95.44%	1093	72.81%	2308	58.45%		
Doctor Web Dr.Web	10	98.94%	6	99.48%	0	100.00%	3	98.80%	19	99.61%	9	98.81%	4	3
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.96%		
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%		4
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Norman Firebreak	0	100.00%	1	99.77%	269	99.12%	12	98.32%	0	100.00%	851	81.55%		
Sophos Anti-Virus	0	100.00%	1	99.97%	0	100.00%	0	100.00%	8	99.80%	10	99.56%	1	
Symantec AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	5	99.54%		1
VirusBuster VirusBuster	0	100.00%	0	100.00%	20	99.77%	11	98.08%	0	100.00%	224	86.17%		

Kaspersky Anti-Virus for NetWare 5.7

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.92%	**False positives**	0

Kaspersky Lab has clearly devoted a little more effort to *NetWare* than many other vendors, providing a full string of *Windows* installer, *ConsoleOne* snapin and web interface. I avoided the last of these, having found the *ConsoleOne* option adequate to get me through the tests, if a little awkward. The X server-based graphical area of *NetWare* has always seemed a little clunky, out of focus and fuzzy around the edges, both visually and in terms of usability. Endless trees of containers within containers, all with complex pages of properties, are confusing and the useful gems are usually hidden away amongst vast heaps of standard-issue options which are often irrelevant to the matter in hand.

The *Kaspersky* pages offered were informative but lacking in controls, which could be accessed via right-click properties tables – that is *if* the appropriate options are available on right-click. This was often not the case, although this may have been the fault of the underlying *ConsoleOne* software and they did mostly pop up on second attempt. With the frustrations of this system recognised if not mastered, the tests were completed without any great upset or surprise. Scanning speeds were somewhat better than expected, with archives not scanned internally by default even in an on-demand scan. Detection figures were as excellent as ever and with no misses and no false positives, *Kaspersky* easily earns itself another VB100 award.

McAfee NetShield for NetWare 4.6.3

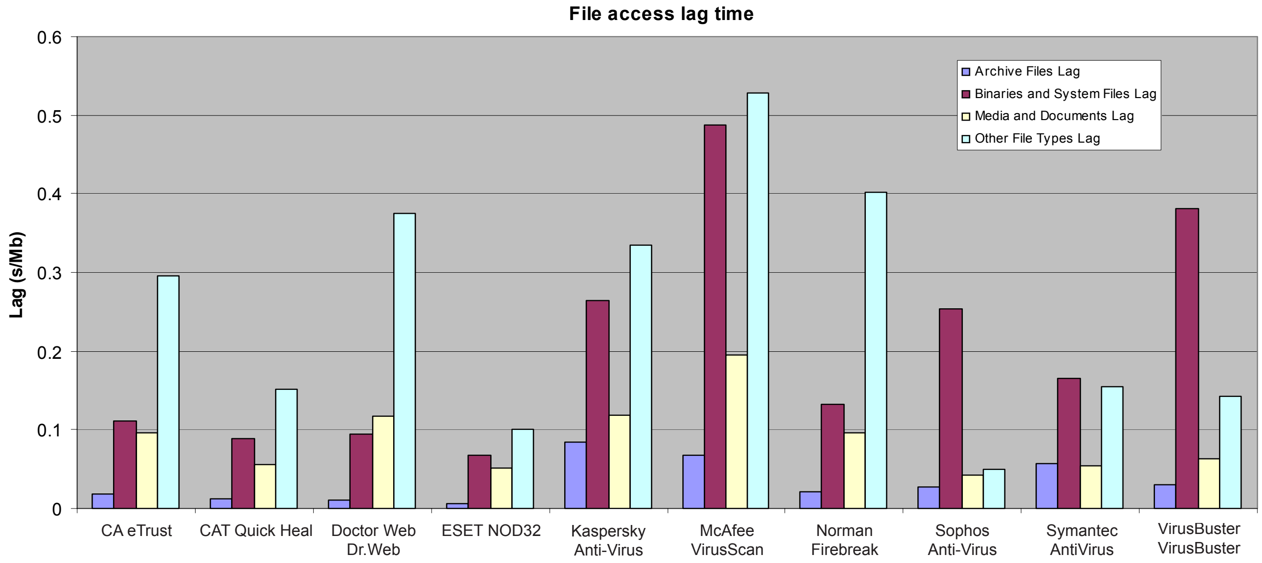
ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

NetShield is another more sophisticated corporate product, with its controls once more on the *Windows* client. Installation takes the form of a simple client-side installer, and the interface is remarkably similar to the familiar *Windows* equivalent – a plain little window with the list of scans and so on in the main part and 'play' and 'stop' buttons available, along with properties and options pages for more detailed configuration.

Scanning times implied thoroughness over haste, particularly when scanning archives on demand, with an impressive number of components discovered and checked. On-access scanning times were similarly lacking in haste over both the executable file set and the miscellaneous files (containing large numbers of small files, which meant *NetWare* itself added some lengthy access time). This thorough approach was fully justified by the detection figures though, which showed flawless detection across the board without a false positive to be seen, qualifying *McAfee* for a well-earned VB100 award.

Norman Firebreak 4.76.2325

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.12%
File infector	98.80%	**Macro**	100.00%
Polymorphic	81.55%	**False positives**	0



Norman again offers a client-based installer. After demanding a lengthy licence key, this seems to run smoothly, with the option of adding the appropriate lines to the autoexec.ncf file to start the on-access protection on system startup. The configuration interface is accessible via both *ConsoleOne* and a plain console screen, although once the settings have been changed via *ConsoleOne* they can no longer be adjusted in the old-fashioned way.

vb Oct 2007 100 VIRUS virusbtn.com

The simpler console-based interface proved more than adequate for my needs, and the tests commenced without difficulty. Detection rates were the same as usual for the product, missing a few of the older samples particularly in the polymorphic set, where the new additions did the product few favours. *Norman* products seem to take objection to the tool used for the on-access test, with some error messages and accompanying beeps flooding the logger screen, even bringing the server to a halt on one occasion. However, several retries brought no repeat of this behaviour, and on the clean sets the errors were not in evidence, and scanning times were excellent. With nothing missed in the WildList set and no false positives, *Norman* earns itself a VB100 award.

Sophos Anti-Virus for NetWare 4.21.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.56%	**False positives**	1

Having spent some time in a previous life being employed to test *Sophos*'s *NetWare* products, I have never found the GUI particularly beautiful or joyous to behold. However, to my surprise, coming towards the end of a necessarily brief but extraordinarily intense spell of testing, the sight of the familiar GUI came as a great pleasure. The fever that had had me shivering at my keyboard all week had just broken when I unzipped the set of files provided onto the test server, typed in 'LOAD SWEEP', and feasted on its blue and yellow marvels. Despite my numerous previous complaints about its clunky, old-fashioned awkwardness, of all the products providing a simple console-based interface this is in fact one of the simplest to operate (although I admit that familiarity could be playing a role here). There are no great expanses of empty space, bizarrely coupled with overlapping windows popping up in one corner, no unnecessary lists of 'yes's and 'no's. The controls reside in one corner, and the remainder of the screen shows status and statistical information about the running of the product, divided sensibly into the major areas.

One fly in the ointment remains in that the path of on-demand and scheduled scans cannot be adjusted, only deleted and replaced – which is often a frustrating procedure given the lengthy pathnames that can build up on servers. A simple typo, or failure to follow the strict syntax required can put some hard typing to waste. Nevertheless, the tests were soon completed without incident, with good times recorded and very solid detection. Again, just a few rare file types were ignored and a handful of the added polymorphic samples missed. However, in the clean sets, a single file was labelled 'Mal/Behav', which is one of *Sophos*'s generic detections indicating suspicious behaviour. In *Sophos*'s corporate market sphere such suspicious files are likely to cause few problems, requiring no more than a judicious decision by a wise administrator to be ignored or

On demand throughput	Archive files		Binaries and system files		Media & documents		Other file types	
	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
CA eTrust	381	6.52	362	6.89	202	7.06	247	2.46
CAT Quick Heal	2473	1.00	270	9.24	108	13.21	146	4.16
Doctor Web Dr. Web	6186	0.40	906	2.75	247	5.77	351	1.73
ESET NOD32	20	124.25	179	13.93	86	16.58	86	7.07
Kaspersky Anti-Virus	7211	0.34	763	3.27	261	5.46	289	2.10
McAfee VirusScan	2184	1.14	1227	2.03	276	5.17	317	1.92
Norman Firebreak	63	39.45	375	6.65	175	8.15	293	2.07
Sophos Anti-Virus	78	31.86	682	3.66	144	9.90	153	3.97
Symantec AntiVirus	1679	1.48	583	4.28	180	7.92	169	3.60
VirusBuster VirusBuster	917	2.71	1035	2.41	85	16.78	76	8.00

left blocked, but where less experienced users are concerned they regularly lead to panic and cause precious un-backed-up computers to be wiped or even, in the most extreme of technophobes, thrown in the skip and replaced. Thus, despite missing none of the WildList samples, under the VB100's strict false positive rules *Sophos* does not make the grade this month.

Symantec AntiVirus Corporate Edition 10

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.54%	**False positives**	0

Symantec's product is another which forms a part of a cross-platform setup aimed at integrating numerous products into a unified whole, and of course the installer runs from *Windows*. This is flashy and impressive, but oddly once it has got through the stage of copying files to the server it pops up a nice friendly message saying 'Now go to the server console and type in "Load Symantec.nlm /install"', or words to that effect. Once this chore is completed, the product can be accessed.

The interface also runs from *Windows* and resembles the normal controls for the *Windows* version. This sped things along nicely, as did the unexpectedly good scanning times, even when running over the infected test sets. Detection rates were as excellent as ever, with only a tiny smattering of the new polymorphic samples missed. Fully covering the WildList, and with no false positives generated in the clean set, *Symantec* more than makes the grade required to achieve a VB100 award.

VirusBuster VirusBuster for NetWare Servers 2.03.014

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.77%
File infector	98.08%	**Macro**	100.00%
Polymorphic	86.17%	**False positives**	0

VirusBuster offered a return to the nice, simple client installer, dropping files onto the server, tweaking the autorun file and starting up the product, which presented another blue screen with some neat little menus for the configuration. These suffered from *VirusBuster*'s standard technique of designing tasks and then running them – less than perfect for my needs, as the tests must be edited for each scan required, but better than some and perfectly usable once a taste for it has been acquired.

Scanning times were in the middle of the field, except over the media and documents set, which consists mainly of *Microsoft Office* files, but my suspicions that this meant

File access lag time	Archive files		Binaries and system files		Media & documents		Other file types	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
CA eTrust	60	0.02	348	0.11	191	0.10	248	0.30
CAT Quick Heal	43	0.01	290	0.09	132	0.06	160	0.15
Doctor Web Dr. Web	39	0.01	306	0.09	221	0.12	296	0.38
ESET NOD32	28	0.01	239	0.07	126	0.05	129	0.10
Kaspersky Anti-Virus	223	0.08	728	0.26	222	0.12	271	0.33
McAfee VirusScan	181	0.07	1285	0.49	333	0.20	389	0.53
Norman Firebreak	68	0.02	400	0.13	191	0.10	312	0.40
Sophos Anti-Virus	80	0.03	703	0.25	113	0.04	98	0.05
Symantec AntiVirus	157	0.06	482	0.16	131	0.05	162	0.15
VirusBuster VirusBuster	88	0.03	1019	0.38	145	0.06	155	0.14

some important file types were being ignored were allayed by some very good detection rates. This accuracy extended over the clean sets, with no false positives generated, although in the archive set access did appear to be blocked to a small number of files with the log file informing the bemused user that the files in question were either corrupted or of unsupported archive types. This quirk does nothing to dent *VirusBuster*'s performance, which amply qualifies for the VB100 award.

CONCLUSIONS

So, another year has passed with no major surprises for users of *Novell NetWare*. It was noted in the last comparative *VB* ran on the platform that products were split into those which kept things simple and pared down and those which tried to gloss things up a bit and provide a more modern graphical experience. If anything, the market seems to have merged towards the middle, with most offering a novice-friendly installer, getting protection up and running with no need for any *NetWare* experience or know-how, and all but the very biggest leaving the fine detail of configuration to those who know their way around the console.

Only one product still required the raw command-line to run on-demand scans, but this lack of attention to surface glitz seemed more than made up for by some even more scorching than usual scanning speeds.

Most of the products made the grade, with one suffering a continuation of a run of bad luck and another brought low by a rare false positive, while speeds showed a fairly broad spread, with the fastest some way ahead of the field and a few lagging noticeably behind. In general, detection rates show a continuation in the general trend of improvement, although the expansion of the polymorphic sets showed that few have yet managed complete accuracy.

Whether *NetWare* will reappear on the *VB* test bench remains an open question. Returning to it after a year, the platform seems even more clumsy and old-fashioned than ever, although that could reflect my inexpert administration more than the services provided by the latest version. It does seem almost inevitable, however, that the platform will fade into the background under pressure from more full-featured, popular and well-supported rivals. Despite its many sterling qualities, after an arduous few weeks battling with it and the products for it (along with a rather nasty bout of flu), I will not be mourning its passing.

Technical details:

All products were tested on 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 *Novell Open Enterprise Server*, *NetWare 6.5 Support Pack Revision 6*. Client machines had *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, all running *Microsoft Windows XP Professional* and *Novell Client 4.91 SP4*.

VB100 NETWARE UPDATE

VB regrets that some erroneous results were recorded for *Symantec AntiVirus 10* in last month's comparative review on *Novell NetWare 6.5* (see http://www.virusbtn.com/pdf/magazine/2007/200710_VB100.pdf). The product was stated to have missed five samples from the polymorphic set – however it has since been discovered that, as a result of file-copying errors, several corrupted samples were included in the test set used to test the *Symantec* product. After removing the corrupted samples and retesting the product, *Symantec AntiVirus 10* was found to detect all files in the set, giving it a faultless 100% detection rating across all test sets.

Virus Bulletin apologises both to readers and to *Symantec* for this error. Measures will be introduced into the VB100 testing process to ensure test sets are kept intact for all tests in future. No other vendors were affected.

[1] Canja, V. Exploiting the testing system. International Antivirus Testing Workshop 2007, Reykjavik.