COMPARATIVE REVIEW

NOVELL NETWARE 6.5

John Hawes

The previous incumbent in this post, Matt Ham, made no secret of his opinion of the *NetWare* operating system and the anti-virus products available for it. Though he left the job exactly one month before the review schedule came back round to *Novell*'s network operating system, this may be mere coincidence. Faithfully following the test timetable laid down before my arrival, I resolved to ignore Matt's cynicism and approach the task with an open mind. Wide-eyed and full of wonder, with the prospect of making friends with the gaggle of strange new AV products before me, I headed into the lab.

PRODUCTS, TEST SETS AND PLATFORMS

One of my first tasks for *VB* was to issue a call for products and to announce deadlines for this test. I chose the date of my first day in the job, 3 July 2006, as the vendors' final chance to submit products and virus data updates, with the WildList deadline a few days earlier; as a result, the In the Wild (ItW) test set was compiled using the April 2006 WildList.

Fortunately for me as much as for the submitted products, there were comparatively few new viruses to add to the test set; while quite a few fell from the list, only around 30 had been added since the *VB* collection was last updated. Along with the handfuls of W32/Mytob and W32/Bagle variants, there were a few variations of W32/Feebs and W32/Lovgate, as well as some names that were new both to me and the list – W32/Nugache, W32/Gurong and W32/Rontokbro are yet more mass-mailing worms with some file-sharing exploitation and backdoor functionality thrown in.

I was also thankful that, for this educational first stab at running *VB*'s comparative testing, a fairly limited selection of products was submitted. I knew practically nothing about most of these products – most of their names and reputations were familiar only from previous reviews in this very publication. As the products arrived, in the form of zipped email attachments, links to FTP sites or descriptions of CDs stashed somewhere deep in the *VB* test lab, I could only wonder what delights and horrors lay ahead of me.

The test machine setup gave me my first real challenge – one in which I quickly conceded defeat. The current version of *NetWare*, 6.5, with the latest Consolidated Support Pack, number 5, is also known as *Novell Open Enterprise Server* (with the support pack renumbered 2). My hopes that the installation CD with the support pack pre-applied would install happily on the shiny new hardware in the test lab evaporated quickly, when it decided it could not begin to cope with the hardware configuration or components. With time pressing, I decided to avoid fiddling about with drivers and such, and installed instead on older, more standard machines, using more powerful hardware for clients. These ran *Microsoft Windows XP Professional SP2*, with *Novell*'s *Client 4.91 SP2* installed. This compromise meant that the *NetWare* servers were running rather close to the minimum permitted RAM, but they seemed to handle it without complaint.

With products gathered, test collections in place and all the machines happily networking and reimaging, I was ready to commence testing.

CA eTrust v7.1 for NetWare (InoculateIT engine 23.72.00, 23.72.57)

ItW Overall	100.00%	**Macro**	99.72%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	99.72%
Standard	99.82%	**Polymorphic**	99.89%

Opting to run through the products alphabetically, I started with *CA*'s offering – perhaps an unfortunate decision as it proved the most time-consuming product to test. Installation of the *NetWare* product took the form of a *Windows* installer, with a simple and fairly helpful GUI taking me through the steps of selecting the target machine and the components to install. Updating was a little more old-school, with a selection of virus data and engine updates copied onto the server manually, overwriting the existing files and requiring a simple unload and reload of the software to be picked up (I later discovered a more sophisticated approach was also available).

Once up and running, I found the interface on the *NetWare* console fairly intuitive, with the top half of the screen displaying status and statistical information, and a menu of options below. A scan of the test set was easily set up and initiated, although there was no option to browse files or save paths. The scan presented me with a screen showing nothing but the path being scanned and the number of files processed, incremented in hundreds. Results finally appeared at the end of the scan, and were written to a log with much of the information about the scan crammed into the lengthy filename.

As I came to the on-access test I ran into trouble. While the console interface allowed me to stop and start real-time scanning, and to examine the status (opening a new screen showing numbers and categories of files scanned and infections found), there seemed to be no way of configuring the scanner's behaviour. The default settings were to 'cure' infected files, with no obvious form of logging. Resorting to

On-access tests	ItW		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust (InoculateIT)	0	100.00%	16	99.72%	1	99.89%	4	99.51%
CA eTrust (Vet)	0	100.00%	12	99.82%	1	99.95%	3	99.84%
Doctor Web Dr.Web	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%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	99.85%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman FireBreak	0	100.00%	0	100.00%	180	91.24%	12	99.45%
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	15	99.30%
VirusBuster VirusBuster	0	100.00%	0	100.00%	124	92.59%	25	99.14%

the manual at this early stage, and browsing through some of *VB*'s previous *NetWare* comparatives, I discovered that configuration could only be effected via an interface on the *Windows* client. This I duly installed, and I found myself faced with a multi-tabbed browser-based 'Threat Management Console' interface. After upping my screen resolution so I could see at least most of the page at once, I navigated my way around some rather baffling pages, and eventually managed to persuade it first to 'discover' and then to control the *NetWare* product. With this hurdle out of the way, I found the interface itself to be fairly easy on the brain.

Testing proceeded without further incident, the product handling the test set quite happily. However, since the *InoculateIT* engine is not the default for the product, it does not qualify for a VB 100% award.

CA eTrust Antivirus v7.1 for NetWare (VET engine 12.06.01 12.06.2285)

ItW Overall	100.00%	**Macro**	99.82%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	99.82%
Standard	99.96%	**Polymorphic**	99.95%

The default Vet engine, while very slightly slower in the throughput tests than the alternative provided, achieved marginally better results in the zoo virus detection, and did just as well in scanning the ItW and clean test sets, earning *CA* its VB 100% award. Switching between the two engines was a simple manoeuvre, involving selecting the appropriate option from a menu; again, while this could be done from the console interface for on-demand scans, the client-based management GUI was required to adjust the on-access component.

Doctor Web Dr.Web for Novell NetWare v4.33.3(.06190)

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

Dr.Web proved a much simpler piece of software, with a large number of tiny virus data files and an NLM copied onto the server and loaded. The console screen presented was a rather murky dark-green-on-black, with a small menu in one corner and most of the screen given over to contact details for the company. The menu itself was simple and logical, with ample configuration options, even offering to detect any jokes I may have had on my machine. On-demand scans were accompanied by a highly detailed information screen.

The product flew through the WildList viruses without difficulty, and did well in the zoo collection too; unfortunately, it claimed one of the clean files was infected with 'Trojan.classic' – an issue which, according to the developers, was fixed less than 24 hours after the close of entries for the test, but one which was sufficient to deny *Dr.Web* the coveted VB 100% award this time round.

ESET NOD32 version 1.1640

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

The simplest of the products by far, *NOD32* provided me with only six files, two of which were basic user guides, while a third formed the EULA. The other three files, once copied to the *NetWare* server, provided a command-line scanner, which merrily zipped through the test set, and an on-access monitor, again with all options passed in as command-line qualifiers. Display and logging were simple and effective, although logs were afflicted with the common problem of truncating long filenames, while speed and detection rates were exceptional.

NOD32 takes the VB 100% award easily in its stride; the only other flaw I could find was on the help screen, entitled 'NOD32 Antivirus System for Nowell Netware'.

Kaspersky Anti-Virus for Novell NetWare v5.60.01

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

Kaspersky Anti-Virus is another product installed from the *Windows* client, with standard *Windows* installer dialogues to select server, apply licences etc. Along with the scanner, a ConsoleOne snap-in and web management tool are offered as optional modules; at least one is required as no control at all is possible from the *NetWare* console. A screen is available on the *NetWare* server, with some statistics and status information, but this is purely for display. The option to add a line to the Autoexec.ncf, causing the product to be loaded on restart of the *NetWare* server, is also offered during the install.

I used the ConsoleOne snap-in which, like all ConsoleOne experiences, tended to suffer moments of extreme slow motion. The snap-in provides tree entries for on-demand, on-access and updating jobs, each with a properties page offering copious configuration options. Scans were simple to set up and run, and the interface fairly intuitive and usable.

With almost total success in the virus scans (the only files missed were in archives, not scanned by default on access to save resources), and no false positives, *Kaspersky* wins yet another VB 100% award.

McAfee NetShield for NetWare v4.6.3

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

Once again going for the *Windows* installer approach, *McAfee* has opted also to provide its own client-side interface. The installer slowed things down by demanding the Java Runtime Environment be available before it would consent to continue; with this in place, the software for the *NetWare* server and the *Windows* GUI installed quickly and easily.

A console screen on the *NetWare* server provides information but no control other than totally unloading the scanner. The *Windows* GUI requires a password to access it, which brought testing to a halt once more – I wrongly assumed it wanted the password for the *NetWare* server, when in fact it had its own, presumably as some kind of second-line licensing technique.

Once access was gained, tweaking the settings was straightforward and speedy. Scanning over the test sets proceeded without incident, and the *McAfee* product, while somewhat on the slow side, was admirably thorough, detecting everything that was thrown at it and deserving its VB 100% award.

Norman FireBreak v4.76.2325

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.48%	**Polymorphic**	91.24%

Norman's *FireBreak* also installed from *Windows*, demanding a lengthy licence key before proceeding. It also required the root of the SYS drive of the *NetWare* server to be mapped to a local drive letter on the client. The installation process mentioned a ConsoleOne-based interface, which I was unable to locate on completion; however, it provided a server console interface too.

There were, in fact, two console screens: the first was a monitor packed with information about real-time scanning, while the other was half-empty, with just a small menu in the top left-hand corner. This provided further menus within menus, all arranged in a fairly straightforward and sensible fashion, allowing me to configure the test scans without difficulty.

On-demand tests	ItW		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust (InoculateIT)	0	100.00%	4	99.72%	1	99.89%	4	99.82%
CA eTrust (Vet)	0	100.00%	12	99.82%	1	99.95%	1	99.96%
Doctor Web Dr.Web	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%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Norman FireBreak	0	100.00%	0	100.00%	180	91.24%	5	99.48%
Sophos Anti-Virus	0	100.00%	8	99.80%	0	100.00%	15	99.33%
VirusBuster VirusBuster	0	100.00%	0	100.00%	124	92.59%	21	99.45%

Once an on-demand scan was started, the details were displayed in another window, while the product chugged confidently through the test set. Although a fair smattering of zoo viruses were missed, nothing in the ItW test set went undetected and the product generated no false positives. As a result, *Norman* also wins a VB 100% award.

Sophos Anti-Virus 4.07.0

ItW Overall	100.00%	**Macro**	99.80%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	99.80%
Standard	99.33%	**Polymorphic**	100.00%

Sophos has done away with its old single-self-extracting-NLM style, and the product now provides a collection of NLMs and data files, much like most of the other products. Once copied to the server and run, the program creates all the folders it needs, demanding a user ID to 'integrate into NDS'. Updating was achieved by dropping identity files into the appropriate folder and reloading, but an automated system is available, administered by a *Windows* console.

The single-screen GUI is fairly straightforward and informative, with a menu top left and the rest of the screen showing stats and figures. One small annoyance was that the path to be scanned could not be edited once entered, and had to be deleted and replaced; this made running separate scans of several folders with the same root path rather frustrating. Another was the truncating of filenames in the log. These minor issues aside, *SAV* detected everything in the wild, threw no false positives, and did very well for speed; a VB 100% award for its performance.

VirusBuster VirusBuster 2006 for NetWare Servers v2.03.006-4.03.012

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.45%	**Polymorphic**	92.59%

VirusBuster, with its handful of NLMs and folder of data files dropped into a folder under SYS:/SYSTEM and added to the search path, demanded a licence key before activating, and then presented me with another uncluttered screen – just a small menu in the centre, surrounded by a sea of blue stripes. I found the controls a little unintuitive at first, with paths for scanning entered under 'Domain management' and scans of these paths initiated from 'Runtime options', but once this was figured out everything seemed to work reasonably well.

This was the only product to cause one of my servers to 'abend' (which was a big surprise to me – in my previous *NetWare* experience this happened fairly regularly). It occurred during some rather cavalier starting and stopping of scans of an entire SYS volume, but despite a few attempts I couldn't get it to reproduce the feat. During the clean set scanning, it also snagged on a file and had to be unloaded quite forcibly. Being in a patient and forgiving

Hard Disk Scan Rate	Executables			OLE Files		Zipped Executables		Zipped OLE Files		Dynamic files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time (s)	Throughput (kB/s)	Time (s)	Throughput (kB/s)	Time (s)	Throughput (kB/s)
CA eTrust (InoculateIT)	222.0	2899.3		12.0	6611.1	122.0	1306.7	27.0	2763.2	30.0	1608.1
CA eTrust (Vet)	248.0	2595.4		13.0	6102.6	110.0	1449.2	29.0	2572.7	23.0	2097.5
Doctor Web Dr.Web	319.0	2017.7	1	19.0	4175.5	106.0	1503.9	19.0	3926.7	35.0	1378.4
ESET NOD32	77.0	8359.1		8.0	9916.7	48.0	3321.2	14.0	5329.1	12.0	4020.2
Kaspersky Anti-Virus	313.0	2056.4		22.0	3606.1	116.0	1374.3	24.0	3108.6	56.0	861.5
McAfee NetShield	433.0	1486.5		50.0	1586.7	257.0	620.3	59.0	1264.5	54.0	893.4
Norman FireBreak	195.0	3300.8		14.0	5666.7	34.0	4688.7	15.0	4973.8	174.0	277.3
Sophos Anti-Virus	164.0	3924.7		14.0	5666.7	53.0	3007.9	14.0	5329.1	23.0	2097.5
VirusBuster VirusBuster	394.0	1633.6	[1]	17.0	4666.7	409.0	389.8	82.0	909.8	78.0	618.5

mood during my first comparative, however, I managed to coax it gently through the rest of the tests. Detection of infected files was solid, with 100% of the ItW samples found, and labelling a single clean set file 'suspicious' was not enough to deny *VirusBuster* its VB 100% award.

CONCLUSIONS

Perhaps thanks to using a combination of the very latest version of the OS and some fairly standard hardware, I experienced few of the problems with *NetWare* that made it the bane of my predecessor's life. Likewise the products, despite a few minor irritants such as the unstoppable sending of *NetWare* alert popups to clients during on-access testing (and the associated incessant beeping), caused few headaches once I came to understand their layout.

I was struck, as Matt has been in previous reviews, by the ever-widening split between the group of products endeavouring to provide an up-to-date, user-friendly experience and those sticking with their tried-and-trusted, simple console interfaces (or, in the case of *NOD32*, the command line). *NetWare* itself reflects this dichotomy, with much of its administration yanked out of the hands of the pared-down console tools and replaced with ConsoleOne snap-ins and web management systems, to the chagrin of many veteran admins and the delight of others.

One interesting anomaly was the contrast in scan rates, and lack of contrast in detection, between the most pared-down and the most idiot-proof products. *McAfee*'s client console is clearly designed to be usable by anyone with a bare minimum of computer skills. This was at the opposite end of the throughput test from the techie-pleasing, command-line-driven *NOD32*, which zipped through the test sets in seconds, while *NetShield* ambled slowly along, way behind the pack. The two were equal top in terms of thoroughness in detecting infections though, with both products missing nothing whatsoever across all test sets.

Detection rates were generally high all round, with developers having had several weeks to get their ItW virus definitions up to speed. With little time available to update the clean test set or expand on the zoo collection, most products' detection rates in the zoo sets had changed little since the last round of tests; nevertheless, as *Dr.Web*'s bit of bad luck shows, false positives can always creep in. It is clear that I will have to get to work improving and expanding the *VB* test sets, in order to give the products more of a run for their money in the next test.

Test environment:

Servers: 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 5, Server version 5.70.05*.

Clients: Identical AMD Athlon 64 3800+ dual core machines with 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, running *Novell NetWare Client version 4.91.2.20051209* installed on *Windows XP Professional SP2*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2006/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

NEARLY VB 100%

In the latest *NetWare* comparative (see *VB*, August 2006, p.15), an unfortunate series of miscommunications resulted in *Symantec*'s product missing the submission deadline. The product has since been run against the test sets and detected 100% of samples in the ItW test set without alerting on any false positives – had the product arrived in time to be included in the comparative review, it too would easily have achieved a VB 100%.