COMPARATIVE REVIEW

Surfing the NetWare

Matt Ham

It is exactly a year since the last *NetWare* Comparative and little has changed. On that occasion I bemoaned the fact that *NetWare* required a 240 MB patch in order to meet *Novell*'s minimum patch list. This time the patch size has increased to 280 MB and must be approaching the size of the operating system itself. The line-up of products has not changed much since a year ago either. There were eleven products on offer in the previous *NetWare* Comparative, all of which are represented again here, along with the additions of *GeCAD*'s *RAV*, which was a beta product last year, and *Trend Micro*'s *Server Protect for NetWare*.

Issues that arose last time fell into two main categories. The first was the age-old favourite of ACG.A and ACG.B in the polymorphic sets, both viruses having caused problems to a wide variety of products over the years. These have, however, become less of a problem with more recent incarnations of software on other platforms and the question is whether this improvement will transfer across to the *NetWare* products on test.

Second was the ever-present bogeyman of extension list problems, one which centred on the lack of scanning where extensionless files were concerned. Since O97M/Tristate is represented in the WildList still, this could prove to be a problem if developers have been tardy. Since the last Comparative there has been yet another new entry as far as extensions are concerned, the .LNK extension which is used by W32/SirCam.A as a method of pretending to be an unadulterated version of the infected and emailed file. This might be expected to prove a pitfall for at least one of the products on offer, if past experience is anything to go by. Past experience also predicts that the victim could be any of those scanners not scanning all files by default, though to discover if this was a problem you will have to read on.

Testing Procedures and Test Sets

By way of a little variation from the previous *NetWare* Comparative, the client platform this time was *Windows 98* with *Novell*'s *Client for Windows 95/98/ME v3.30.00.0 SP 3* running on W98. *NetWare* itself was version 5.1 patched to Service Pack 3. This patch level adheres to the *Novell* minimum patch list for the week of product submission. Products were submitted no later than 6 August, and the July WildList (the most recent available at that time) was used as a basis for the construction of test sets for the In the Wild (ItW) set.

Scanning was performed on the server with the virus test sets and speed test sets both being located on the SYS volume. While this avoids scanning speeds being dictated by the network speeds under the test conditions used, it may give higher throughput rates than might be encountered when scanning files across a network.

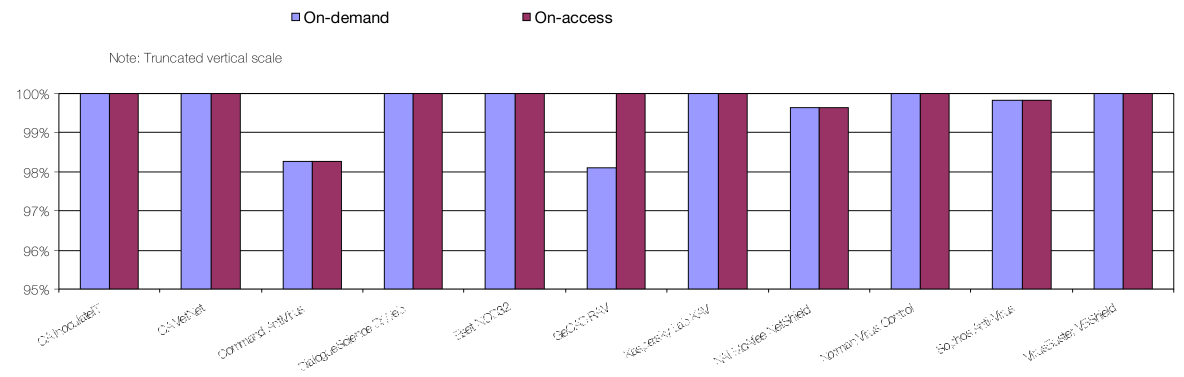
For the on-access scanning test the files in the viral test set were opened from a client machine in order to trigger detections. Due to the nature of server scanning on *NetWare* the checking of boot sector viruses was not performed.

There were a few additions to the ItW test set. The most notable newcomer was the aforementioned W32/SirCam.A with its wide selection of double extensions and the usual addition of 32-bit *Windows* infectors, script worms and macro viruses making up the unexceptional remainder.

Symantec

The offering from *Symantec* showed early promise but was soon discovered to be virtually untestable in the defined test environment. The NLM-based portion of the product can readily be installed and updated, though the latter involves some shenanigans, from a *Windows 98* Client. At this point there is a *Norton AntiVirus* available on the server, but how is it controlled? The answer is in the use of *Symantec*'s

In the Wild File Detection Rat



On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number Missed	%	Number Missed	%	Number Missed	%	Number Missed	%
CA InoculateIT	0	100.00%	0	100.00%	9	98.90%	0	100.00%
CA VetNet	0	100.00%	16	99.71%	1	99.99%	0	100.00%
Command AntiVirus	7	98.27%	0	100.00%	1	99.99%	6	99.42%
DialogueScience DrWeb	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	1	99.98%
GeCAD RAV	8	98.10%	0	100.00%	0	100.00%	17	99.13%
Kaspersky Lab KAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI McAfee NetShield	6	99.65%	3	99.97%	1	99.88%	8	99.77%
Norman Virus Control	0	100.00%	0	100.00%	17	97.92%	14	99.58%
Sophos Anti-Virus	3	99.82%	13	99.67%	191	95.36%	37	99.15%
VirusBuster VBShield	0	100.00%	39	98.97%	28	95.71%	17	99.37%

proprietary management interface, which works solely via *NT*. With a *Windows 98* Client no control could be exerted upon the server software and testing was abandoned.

Trend Micro

Trend's offering too declared itself to require *NT* as an administration platform, though the claim here was that after installation from an *NT* box, the server side software could be controlled through *Windows 98*. Several hours later, having set up a number of information servers in order to deploy the *Trend* product, the situation was much the same – a loaded, but singularly uncontrollable NLM on the server. Again, testing was abandoned.

Computer Associates InoculateIT v 4.5 engine 26.04

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	100.00%	Polymorphic	98.90%

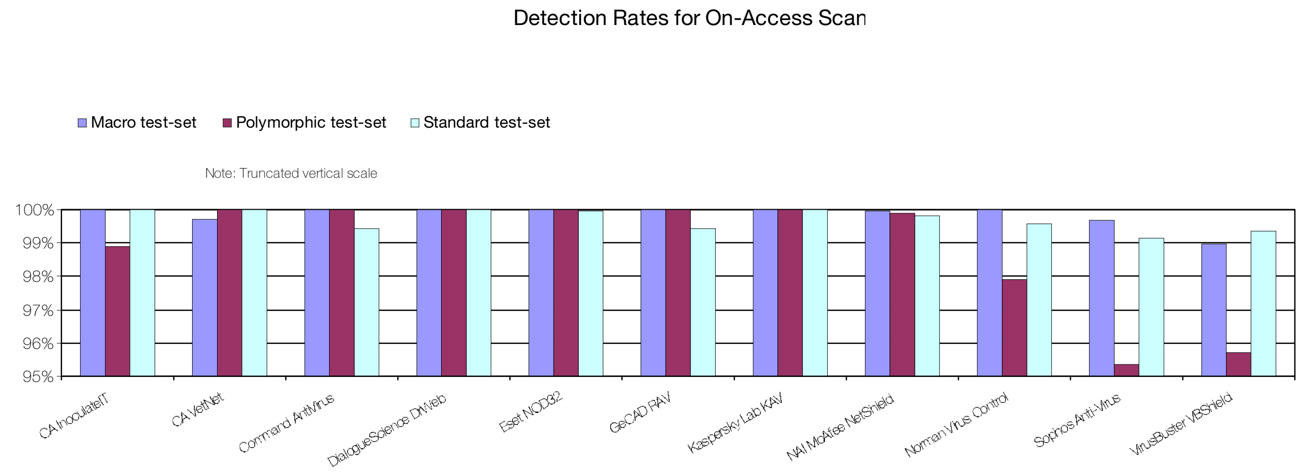
Despite having the same version number as in the last Comparative, *InoculateIT* has seen changes in many parts of its operation. Installation uses the same CD as the last test and, as is customary with *InoculateIT*, there was a patch to be added before operation could begin. These processes performed with admirable ease, though updating virus signatures was more basic and labour-intensive.

Amusement was to be had when loading and unloading the software with the use of the surely made-up word 'endingizing' during one particular session. Notification of infection messages with hex descriptors commencing 0baddeed was also sufficient to enliven the testing procedure a little. If faults were to be found, these would be in the fact that the test procedure took an inordinately long time – delays were noted during the clean set at every point where the directory to be scanned was altered.

On the detection results front, however, *Computer Associates* will be pleased again with only nine samples of the polymorphic W95/SK.8044 being missed out of the full test set. As expected from past performances there were no false positives in the speed testing, so *InoculateIT* is once more possessor of a VB 100% award.

Computer Associates Vet NetWare Anti-Virus 10.3.4

ItW File	100.00%	Macro	99.71%
ItW File (o/a)	100.00%	Macro (o/a)	99.71%
Standard	100.00%	Polymorphic	99.99%



In the last review, the *VetNet* program was considered one of the simplest for installation. There was a little confusion as to the name of the program; although referred to almost exclusively as *VetNet*, the actual NLM goes by the name of *Vet_Net* – something which, thankfully, was explained in the HTML installation file provided. After this the program proved easy enough to configure, and the scans were rapid enough that any installation delay could be easily forgiven.

Configuration changes are implemented at the console rather than at an external point such as the workstation, and therefore did not incur a delay in registering, making this a pleasant affair as far as direct hands-on use is concerned (though, perhaps, less desirable to a remote administrator).

As far as detection was concerned, *Vet* missed identical files on access and on demand, one of which was a single specimen of the polymorphic virus ACG.A. The remainder of misses lay in the macro set, where the majority of misses were samples of the polymorphic X97M/Soldier.A. The misses were very similar, in fact, to those in the DOS Comparative two months ago, and were a vast improvement over the detection rate noted in the September 2000 *NetWare* comparative. A good improvement since last year and retaining full detection of In the Wild files gains *Vet NetWare* a further VB 100% award.

Command AntiVirus for NetWare v 4.61I

ItW File	98.27%	Macro	100.00%
ItW File (o/a)	98.27%	Macro (o/a)	100.00%
Standard	99.42%	Polymorphic	99.99%

Unusually, *Command* is the sole representative of the *F-Prot* stable represented in this review and the absence of its usual pair of running mates seemed to have put it off its stride. The main problem lay in detection, which was far from *F-prot*'s usual outstanding performance on other platforms and had reverted to the singularly inept manner in which it performed in the last *NetWare* Comparative. On that occasion a VB 100% award was missed by the absence of extensionless files on the list of those to be scanned. Rather than learn from this experience, *Command* now fails to scan .HTM, .PIF and .LNK extensions by default. This combination saw many samples of JS/Kak missed, a scattering of ignored VBS viruses with HTM portions and a failure to detect some of those files infected by W32/SirCam.A.

On the administration front, *Command* scored some negative marks by having a far too vigorous scheduled scan which seemed difficult to be rid of, and which interfered with several test procedures. Since scans are still somewhat tricky to spot as being in progress this was not noted at the time of scanning. The scanning speeds were also very much on the slow side and *Command* will, no doubt, be somewhat disappointed with their overall performance.

The cynical, and highly controversial hypothesis that the lack of any other *F-Prot* products in this test might be due to the other developers being well aware of its failings and preferring to be kept out of the public eye is, of course, totally unsubstantiated since neither product was inspected in any way.

DialogueScience DrWeb for NetWare v 4.25

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

The *DrWeb for NetWare* installation process is one of the simpler of those on offer. Simply unzipping the files that make up the product into an appropriate directory enables activation – though setting up a path to that directory in addition will make running the program simpler in the long run. Scanning was the simplest and speediest in completion of any of the products examined up to this point. Although others may find snap-ins and the availability of an aesthetic interface important, to a jaded reviewer's eyes speed and

On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number Missed	%	Number Missed	%	Number Missed	%	Number Missed	%
CA InoculateIT	0	100.00%	0	100.00%	9	98.90%	0	100.00%
CA VetNet	0	100.00%	16	99.71%	1	99.99%	0	100.00%
Command AntiVirus	7	98.27%	0	100.00%	1	99.99%	6	99.42%
DialogueScience DrWeb	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	1	99.98%
GeCAD RAV	0	100.00%	0	100.00%	0	100.00%	13	99.42%
Kaspersky Lab KAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI McAfee NetShield	6	99.65%	3	99.97%	1	99.88%	4	99.84%
Norman Virus Control	0	100.00%	0	100.00%	17	97.92%	14	99.58%
Sophos Anti-Virus	3	99.82%	13	99.67%	191	95.36%	37	99.15%
VirusBuster VBShield	0	100.00%	39	98.97%	28	95.71%	17	99.37%

simplicity bring greater pleasure. There will, of course, be a need for greater administrative ability in a large organisation (though with *NetWare* products this may well be less of an issue than for non-server operating systems, since the smaller number of such machines makes home-made scripts much more of a feasible deployment method).

The suspicious file problem, consistently the only fly in *DialogueScience*'s ointment, is still present but not alarming. As for detection, this was once again at the 100% level in all test sets and as such can not be faulted. *DrWeb* rightly earns a further VB 100% award to add to its collection.

Eset NOD32 v 1.99

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	99.98%	Polymorphic	100.00%

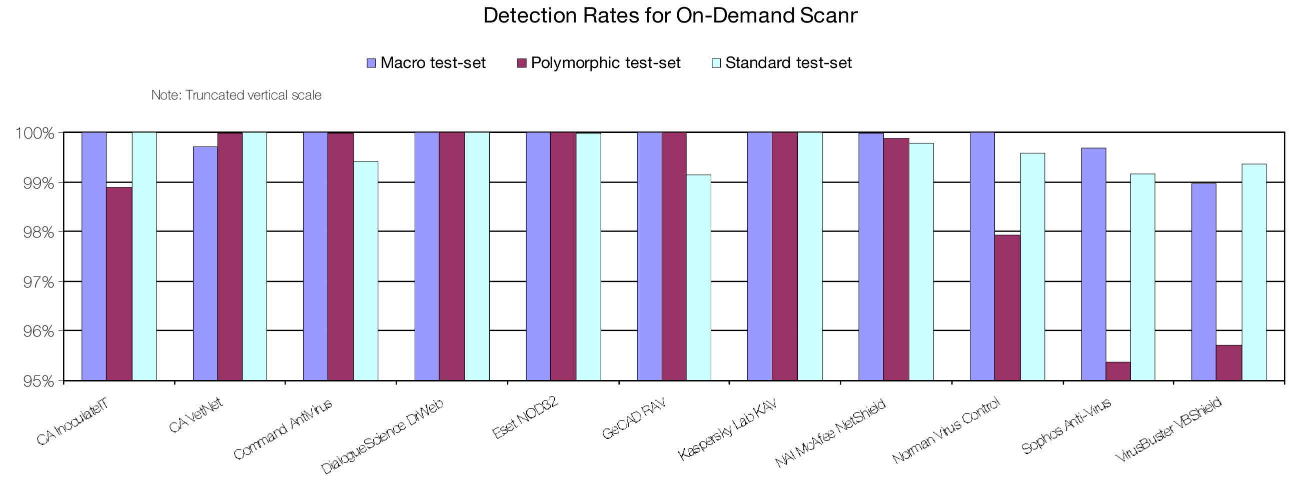
NOD32 has similarities to *DrWeb*, and not only in the length of its product name. The product is another which has a more basic than average interface – in this case consisting of a command line-invoked scanner for both on-access and on-demand duties. These share the same virus database information and lack any form of aesthetic adornment. However, these functional lines conceal what is by far the fastest of the scanning engines in this review. The fastest of the other products was more than twice as slow as *NOD32* over the clean set of executables, while the slowest was over 40 times as tardy.

This was remarkably similar to *NOD32's* performance in the review a year ago, as was the number of files missed. On that occasion one file was missed in the standard set, and on this occasion the standard set saw another solitary miss – though, admittedly, on a different virus. No false positives were registered and thus *Eset*'s product is the happy recipient of a VB 100% award.

GeCAD RAV Antivirus v 8 1.00

ItW File	98.10%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	99.13%	Polymorphic	100.00%

Differences between on-access and on-demand scanning were rare in this review, though, unlike the last *NetWare* review, not non-existent. The greatest extent to which this was seen was in *GeCAD*'s product. A very good performance in on-access scanning was somewhat let down by several misses on demand In the Wild. These were all found in VBS worms, both in the .VBS and .HTM parts of these samples.



Unfortunately the log file produced by *RAV* was unusable for parsing attempts and thus detection on demand was completed by deletion. On-access scanning, on the other hand, was performed by denial of access – though it seems unlikely that this might be the cause of such a difference in performance. A difference in behaviour between on-access and on-demand scanning is perhaps not that surprising however, since this is another product which has two applications, one for on-demand and another for on-access scanning. These both operate as console-style GUIs on the server and clearly this has led to slightly differing configurations between the two.

In the last *NetWare* test this version of *RAV* was only just out of beta and failed to install, so these results are a pleasant surprise in comparison. Since the In the Wild on-demand misses are clearly reparable by dint of being absent on access, the future looks promising for the product. The only possible problem lies in the speed of scanning, which was somewhat tardy on the clean executable set, though this is balanced by much superior speed on the OLE set.

Kaspersky Anti-Virus for Novell NetWare 3.06.04

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

Kaspersky Anti-Virus performed well and was easy to install in the last *NetWare* review, making its behaviour in this review all the more mystifying. The NWAdmin portion of the program was able to load the NLM onto the target server, but failed to realise that it had done so. Many hours of parameter and protocol adjustment succeeded in tracking down the problem – AVP being the only product that requires TCP/IP communication to be successful, and being very fussy about the port it performs this over. This problem overcome, the product was one of the simpler to operate, with a large degree of control available in a rather simpler manner than with most other products. The scans proceeded speedily both on access and on demand, though results were at first somewhat confusing. There was a clean sweep on all files, but installing an optional upgrade removed detection of the W32/SirCam samples in the WildList. Thankfully for *Kaspersky Lab*, this was mentioned nowhere in the documentation and was thus not considered to be a default option.

So, despite these various odd features thrown by fate into the path of testing, *Kaspersky Anti-Virus* earns a VB 100% award. As for speed testing the product falls in the middle of the pack – though faster than average for a product controlled from the client rather than the server.

Network Associates McAfee NetShield v 4.50

ItW File	99.65%	Macro	99.97%
ItW File (o/a)	99.65%	Macro (o/a)	99.97%
Standard	99.77%	Polymorphic	99.88%

The installation of *NetShield* proved one of the more taxing, in that it seemed to crash without respite whenever installation was selected. Thankfully it turned out that the installer was simply excruciatingly slow, to an extent not seen with any other product.

The *McAfee* interface on the *NetWare* machine is among the most cluttered of all those on test – combining results for both on-demand and on-access scanning on one standard-sized page. This does not particularly hinder control, but does leave the user somewhat cross-eyed. This is mitigated to a certain extent by the presence of the client-based program, which allows for control over the scanning operations.

On the other hand, this client-based program is apparently in constant contact with the server, resulting in slow scanning speeds if viruses are detected. Admittedly the information seems to be bundled up – since information about infections is incremented in steps rather than on a file-by-file basis, on both server and client.

Hard Disk Scan Rate	Executables			OLE Files		
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]
CA InoculateIT	1181	463109.4	0	69	1149764.7	0
CA VetNet	275	1988844.3	0	25	3173350.7	0
Command AntiVirus	1725	317062.1	0	103	770230.7	0
DialogueScience DrWeb	354	1545006.1	[16]	26	3051298.7	0
Eset NOD32	102	5362080.1	0	14	5666697.6	0
GeCAD RAV	1841	297084.3	1 [1]	18	4407431.5	0
Kaspersky Lab KAV	509	1074522.9	0	40	1983344.2	0
NAI McAfee NetShield	922	593201.9	0	48	1652786.8	0
Norman Virus Control	4414	123908.5	0	20	3966688.4	0
Sophos Anti-Virus	325	1682868.2	0	37	2144155.9	0
VirusBuster VBShield	707	773595.7	0	92	862323.6	0

With regard to detections, however, *NetWork Associates* have once again managed to be caught out by the pesky problem of scanned extensions. The fact that relatively new entries .PIF and .LNK files went unscanned came as no great surprise, but a weary sigh is all that can be mustered upon noting that extensionless files were not subjected to examination. Since the files used in this test were those most recently downloaded from the *NAI* Web site, not even the excuse of the use of old media can be claimed in defence of the guilty parties.

NetShield is of note as a rather obvious sign of the lack of change in some of the programs evaluated here. All the notable problems seen in this review were similarly noted in the previous review – a year may be a vast aeon in politics, but in *NetWare* anti-virus it can sometimes seem like a fleeting second.

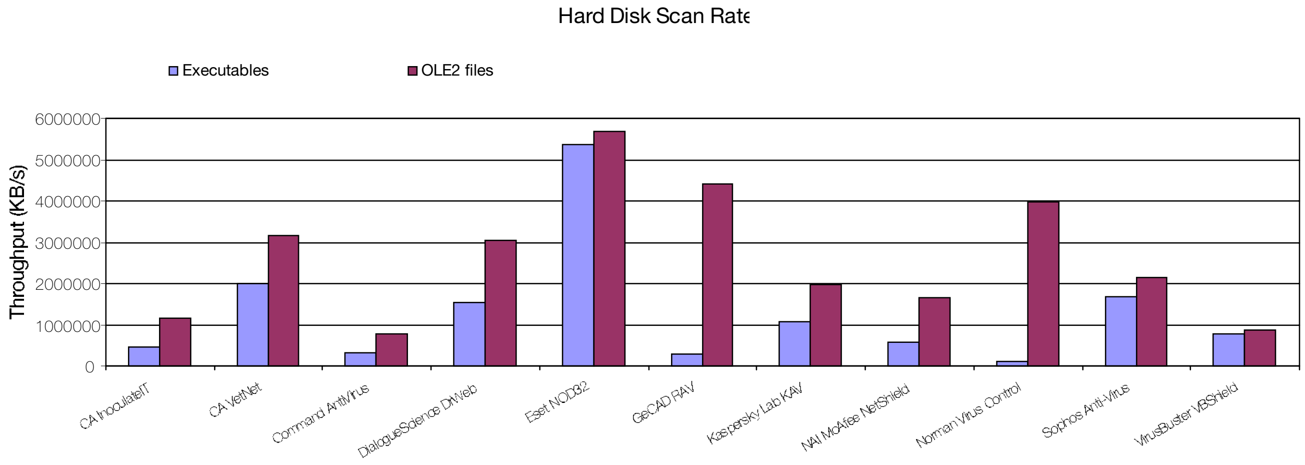
Norman Virus Control v 4.05

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	99.58%	Polymorphic	97.92%

Norman Virus Control suffers from some identity problems, being referred to alternately as *FireBreak* and *NVC for NetWare* in the documentation and installation programs. Commencing with installation the user is directed to NWAdmn32 which is now the place in which configuration is performed. This has the odd side effect of making it impossible to alter settings for *Norman Virus Control* from the program itself – all such commands must be issued from this adminstration program. Part of the installation process had to be performed manually from NWAdmn32 but overall the process was not too complex.

As far as the false positives test was concerned, there was one major glitch in that the scan process froze repeatedly on several of the files in the clean set. Time did turn out to be the great healer in this matter, but scan times were markedly increased as a result, producing the slowest scanning of executables in the clean set by quite a margin. The OLE file scanning was not afflicted by this problem, neither was the viral test set to any noticeable degree.

Norman's polymorphic detection rates were well up on last year's performance, in accordance with other platforms for



the *Norman* product range where engine overhauls have been made across the board. These improvements are certainly good to see and result in a VB 100% award.

Sophos Anti-Virus v 3.48

ItW File	99.82%	Macro	99.67%
ItW File (o/a)	99.82%	Macro (o/a)	99.67%
Standard	99.15%	Polymorphic	95.36%

The *Sophos Anti-Virus* NLM retained the idiosyncrasies that make it somewhat less than pleasant to review, the most irksome of which are the small maximum size of log file and an inability to select sets of files easily for scanning using the installed list of program extensions. This list of extensions also proved to be the program's weak point as far as detections were concerned, since the .LNK and .BAT versions of W32/SirCam.A went undetected. The requirement for extra extensions to be added to the list has been added to the information in the IDE virus definition file compilations on the *Sophos* Web site, though unfortunately this innovation came too late to save company pride on this occasion.

Other than these rather problematic misses detection was elsewhere somewhat hindered by extension-related misses and those files not detected due to the overheads involved. One area where the *Sophos NLM*, and other *Sophos* products in general, still have problems due to detection-related issues is the polymorphic set where ACG.A still remains undetected.

VirusBuster VBShield for NetWare v 1.09

ItW File	100.00%	Macro	98.97%
ItW File (o/a)	100.00%	Macro (o/a)	98.97%
Standard	99.37%	Polymorphic	95.71%

And so to the last of the products on review this month. This was a 'hiccupy' newcomer in the last *NetWare* review, so its behaviour comes under careful scrutiny. The readability of report files seemed to have improved when displayed on-screen, though this initial improvement proved to be short-lived and detection was again performed by deletion.

The detection rate was where the majority of improvements lay, and these were vast indeed. None of the percentage detections in any category were above 96% in the previous review, with polymorphic viruses coming in at a lowly 77% rate. On this occasion the polymorphic detection rate is vastly improved with marked increases in the ItW test set – sufficiently improved, in fact, to warrant a VB 100% award. This increase in detection rates is certainly not a one-off occurrence either: it was noted in last year's *NetWare* review, and if it continues into the future more VB 100% awards are almost certain to follow.

Conclusions

As this test draws to a close, I ponder the comments made at the end of the last *NetWare* review. My conclusion is brief: the situation has not remained as dire as it was at the end of the last *NetWare* review. Improvements have been made by many products. Then again, there remain some odd behavioural traits in products which veer towards the sadistic. I suspect I shall be able to say exactly the same next year.

Technical Details

Server: 500 MHz AMD Athlon server with 6 GB HD, 64 MB RAM, CD-ROM and 3.5-inch floppy running *Novell NetWare* 5.11 with Service Pack 3.

Workstation: 750 MHz AMD Duron workstation with 128 MB Ram, 8 and 4 GB dual hard disks, CD-ROM, LS120 and 3.5-inch floppy, running *Windows 98* with *Novell Client for Windows 95/98* version 3.30.00.0 Service Pack 3.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2001/07test_sets.html.

A full description of the results calculations protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.