COMPARATIVE REVIEW

NetWare and Tear

Matt Ham

The annual *NetWare* comparative has arrived once more and, as is usually the case, a new version of *NetWare* is in order; this year *NetWare 6* replaces *NetWare 5*.

The GUI that was introduced in *NetWare 5* has been retained in *NetWare 6*, although this is of limited relevance since the majority of products in this review are console-based. The minimal need to use the interface came as something of a relief, since *Novell*'s style gurus have opted for an interface which depicts a number of people in irritatingly unnatural poses who seem to have been attached to *Novell*'s trademark red 'N' by cut-and-paste jobs of varying degrees of competence.

Platform Scares

It seems that the choice of *NetWare 6* as a test platform scared off some vendors, who did not feel that their products had been adequately tested on the operating system to allow them to be subjected to the full *VB* testing process.

Special mention on this front goes to *Symantec*'s *Norton AntiVirus*. Originally this was submitted for testing in its 7.60 Corporate Edition version. However, it soon became apparent that there were some problems with the product's on-access scanning.

A discussion with *Symantec*'s engineers revealed that the product had been submitted under the misunderstanding that the test would take place on *NetWare 5*. Since the 7.60 version of *NAV* is not designed for *NetWare 6*, the product was withdrawn from the review. Unfortunately, version 8 of *NAV*, which *is* designed for *NetWare 6*, is not yet commercially available and so could not be included in the test.

Test Sets

Changes in the test sets for this comparative included the addition of W32/Simile (aka W32/Etap) in order to bolster the ranks of the polymorphic set. Since polymorphics and extensions were the root of some problematic issues in the previous two *NetWare* reviews, these were of particular interest on this occasion.

The last *NetWare* comparative review (see *VB*, September 2001, p.17) predicted that this year's review would prove to be much the same as ever – in that improvement would be seen in the general behaviour of the products, but that idiosyncrasies would remain to torment the unlucky user (and cause them to damn *Novell* and its assembled developers unto the seventh generation).

Since the proof of this metaphorical pudding is in the eating, it is now time to tuck into the offerings on the table, and judge them as sweet, savoury or downright sickening.

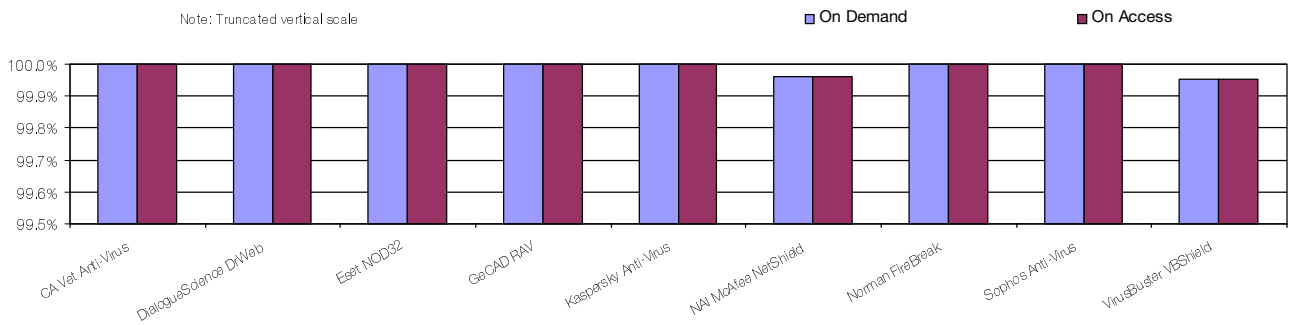
Test Environment

The test equipment has changed considerably since the last *NetWare* review in terms of both hardware and software. The configuration chosen was a *NetWare* server with an *NT* client. (In the last comparative several products demonstrated an incompatibility with a *Windows 98* client and as a result *NT* or, more likely, *XP* client is likely to be used in future reviews.)

While on-demand scans were selected to be performed entirely on the server where possible, control of this scanning was initiated by client-side utilities in cases where these were provided. Wherever possible, results are obtained by the parsing of log files – only one product in this review required different treatment.

On-access scanning was tested using file access from the client to files located on the server. This access was

In the Wild File Detection Rates



On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA Vet Anti-Virus	0	100.00%	16	99.71%	13	99.31%	1	99.94%
DialogueScience DrWeb	0	100.00%	34	99.20%	1	99.96%	1	99.98%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	78	95.29%	6	99.67%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	2	99.84%	0	100.00%
NAI McAfee NetShield	1	99.96%	3	99.97%	1	99.92%	2	99.88%
Norman FireBreak	0	100.00%	0	100.00%	149	91.25%	15	99.32%
Sophos Anti-Virus	0	100.00%	9	99.77%	93	93.31%	17	99.43%
VirusBuster VBShield	1	99.95%	0	100.00%	658	86.87%	11	99.56%

triggered by a custom utility which performs file opens on every file in the virus test sets. Products were logged as able to detect a virus on access if, when configured to do so on viral detection, the files were blocked from being accessed.

Logging for on-access scanners is still less well implemented than for on-demand scanners and thus this method has been chosen as being more universally applicable to the products on test. Again, there was one product that could not be tested in this way, instead detection was judged by deletion of infected files.

Try, Try and Try Again

Where results were unobtainable due to software failure or displays of particularly strange behaviour of the software, the testing procedure was repeated up to three times so as to determine whether the defect was reproducible or simply a one-off glitch.

Despite the fact that the images used for these new installations are identical in every way, this process of repetition will often change the results obtained. Products which remain untestable after three retries are noted as such. Although, in the past, more than three attempts have been required to coerce a product into correct operation, this cut-off point has been introduced due to the time constraints imposed by publication deadlines.

The server operating system was *NetWare 6* with service pack 1 installed, linked by a 100 Mbit ethernet connection to an *NT 4 SP 6* workstation. The client software used on the workstation was *Novell Client 4.83*. Both the workstation and the server were fully re-imaged between changes of product, ensuring that each product had an identical configuration for installation. A further *Windows XP Professional* workstation was attached to the server for use in storing results data. Hardware specifications are provided at the end of the review.

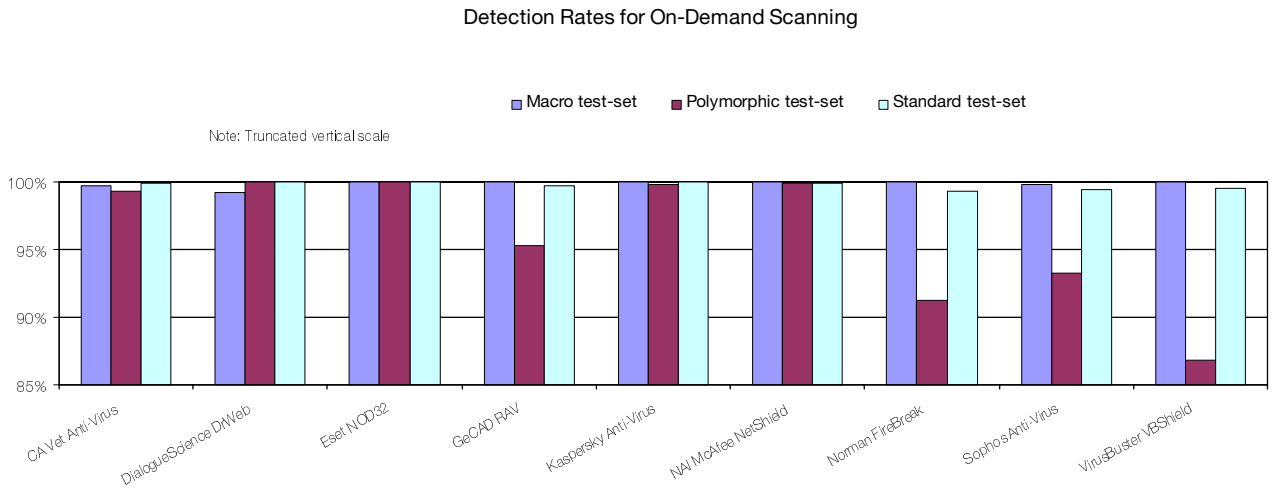
The method of control varied considerably between the products reviewed, although the majority were controlled directly through the NLM on the server. This method of control should be assumed throughout the review unless otherwise stated. Where required, NWAdmin version 5.1.9f was installed for administrative purposes.

False Positives and Archives

Testing of false positives was performed on the usual *Virus Bulletin* clean set, consisting of 5500 clean executables and a selection of OLE files embedded with varying numbers of macros and other OLE streams.

For the testing of archive handling, subsets of the aforementioned test libraries were used, zipped into multiple archives with one level of compression applied. Figures for scanning throughput on the archived file sets are given for the uncompressed content size of the archive.

In products which are speed-limited by disk access times, throughput may be higher on archived files than on the same files when unarchived. This is due to the fact that the time taken to read an archive plus perform calculations to decompress the archives in memory can be faster than reading a much larger file from the hard drive.



Computer Associates Vet Anti-Virus 10.4.9 v 2160

ItW File	100.00%	Macro	99.71%
ItW File (o/a)	100.00%	Macro (o/a)	99.71%
Standard	99.94%	Polymorphic	99.31%

Vet is usually among the first products to be described in the writeup of any comparative, and on this occasion it was also the first product to undergo the testing process. The first test always sets the tone for a review, since although certain products may be uniformly easy or difficult to review, the operating system in use can be gauged fairly quickly for quirks and oddities. As mentioned above, this was a pleasant experience with *NetWare*, allowing the products themselves to claim the rightful centre of attention.

Installation of *Vet* was straightforward, and updating was a simple matter of copying across new files into the installation directory.

Leaving aside the mention of Aardvarks in the manual, *Vet for NetWare* has no major distinguishing features, its interface being a single central NLM with a classic *NetWare* look. Irritatingly, the status of a scan cannot be viewed from this interface – the only information available is the fact that the scan is in progress. Since the log files are locked during scanning this leaves an air of mystery surrounding any scan. This obfuscation also applied to some of the options within the program where, for example, the default state of archive scanning could be discovered only by scanning.

Despite these complaints, *Vet*'s performance was good – scans were fast and false-positive-free on the clean set and no misses of virus samples In the Wild gains the product a VB 100% award. Where weaknesses did occur in detection they were isolated rather than general – with the polymorphic viruses in both polymorphic and macro test sets containing some files which presented difficulties.

DialogueScience DrWeb 4.28

ItW File	100.00%	Macro	99.20%
ItW File (o/a)	100.00%	Macro (o/a)	99.20%
Standard	99.98%	Polymorphic	99.96%

Also sporting a classic *NetWare* look, *DrWeb* emphasises its retro style by using a green colour scheme for the interface. The most unusual feature of the product is its total lack of an on-demand scanner. This is not the fatal flaw that might be anticipated, since scheduled scans may be used as a replacement for this functionality. However, the process of on-demand scanning is rendered somewhat clumsy by this design. The scheduled and on-access scanning portions of the program are both controlled from a single NLM.

Scanning of the clean test sets was at the faster end of the spectrum, with the usual 16 suspicious files being produced. With full detection of files In the Wild, *DrWeb* earns the second VB 100% award of this comparative. The newer polymorphics were a particularly strong area for *DrWeb*, with only one sample missed in this category. Slightly more surprising was a weakness in older Excel macro viruses.

Eset NOD32 1.280 20020708

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

When discussing *NOD32* in the past, faults have been few and far between, but on this occasion the matter was somewhat different. The normally delightful *NOD32* log file has, in some bizarre fashion, been converted to a festering mass of corruption designed to attract dire imprecations.

First, the file names in the log were changed to 8+3 format, making it extremely difficult in some cases to determine

On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA Vet Anti-Virus	0	100.00%	16	99.71%	13	99.31%	3	99.81%
DialogueScience DrWeb	0	100.00%	34	99.20%	1	99.96%	1	99.98%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	78	95.29%	8	99.55%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	2	99.84%	2	99.87%
NAI McAfee NetShield	1	99.96%	3	99.97%	1	99.92%	4	99.76%
Norman FireBreak	0	100.00%	0	100.00%	150	91.25%	15	99.32%
Sophos Anti-Virus	0	100.00%	13	99.67%	93	93.31%	18	99.41%
VirusBuster VBShield	1	99.95%	0	100.00%	664	86.74%	13	99.44%

exactly which files had been missed. As if that cardinal sin were not enough, the path delimiting '\' symbols were all converted to '/' and all file names converted to lower case. While the changing of path delimiters may be excusable for some arcane *NetWare*-specific reason, it seems pointless to change file names in two respects when referring to those files in a log.

Returning to the product, *NOD32* comes as two NLMs – amon and nod32 – handling on-access and on-demand scanning respectively. Installation and update were both simple matters of copying the files to the correct location. The nod32 NLM is loaded and unloaded each time an on-demand scan is initiated and, as such, does not support scheduled scans directly.

As far as detection and scan speeds were concerned, *NOD32* retained its impressive performance history, detecting all files in all test sets. This, combined with no false positive detections, gains *NOD32* yet another VB 100% award. It is to be hoped that the new-found log file problems remain less of an ongoing feature than the product's impressively high detection rates.

GeCAD RAV AntiVirus v.8 1.07

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	99.67%	Polymorphic	95.29%

RAV is the first of the products described so far to have a *Windows*-based installer for its product. An automatic update function is supported, though for full automation it seems that the *Windows* product must also be installed. The product itself is split into separate components which are loaded as different NLMs for each function.

The scan of the clean sets was notably slower on the executable files than the OLE files in the test set, and resulted in one false positive. The rate of scanning on clean files was also significantly slower than that on infected files – which would suggest that *RAV* is using quite a large quantity of heuristics.

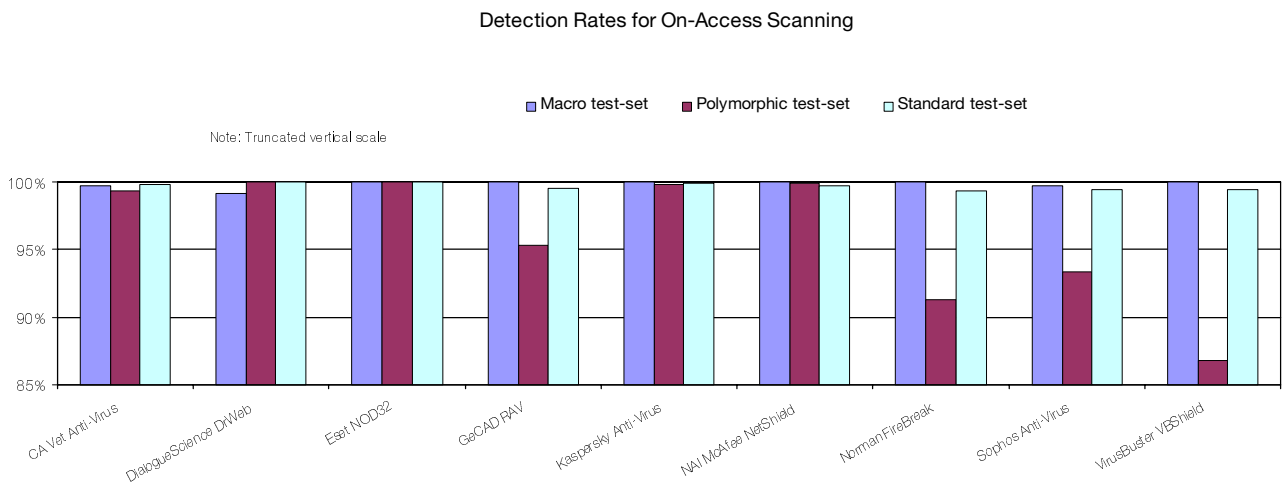
The single false positive will be irritating for *GeCAD*, since the detection statistics for *RAV* were good. Misses did occur on the polymorphics in both the polymorphic and standard test sets, but samples in the macro and ItW sets were fully detected.

The two main misses were the newer polymorphics of W32/Etap and W32/Zmist.D. This pair is rapidly assuming the mantle long held by the ACG and SP variants in the category of 'difficult-to-detect' polymorphics.

The matter of log files reared its ugly head again when analysing *RAV*'s results, the path names having been converted to 8 + 3 format in the log.

Kaspersky Anti-Virus 4.00.01

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	99.97%
Standard	99.09%	Polymorphic	98.10%



Kaspersky Anti-Virus is the first of those products tested which does not rely on being controlled directly through the NLM or a command line interface. During installation it installs snapins for both NWAdmin and ConsoleOne and requires that all administration be performed through these.

In this case, NWAdmin was used for control of scans. For this method of administration there are both pros and cons. On the negative side, there is the need for communication between the client and server during scans, which might be expected to lead to slower scan speeds. In practice, however, the scans were not noticeably slower than those performed by other products, so this is a niggle of minor concern. On the more positive side, the use of a real GUI rather than a *NetWare*-style console interface makes both administration and scans substantially easier to perform.

Scanning performance was flawless in the In the Wild and macro test sets which, combined with a lack of false positives, results in a VB 100% award for *Kaspersky* after a considerable drought. There were misses in the standard and polymorphic sets, which were, oddly enough, confined to samples whose file names begin with the letter N.

This odd behaviour was apparent in both on-access and on-demand tests, but further examination of the results showed that the phenomenon was not exhibited on the same files in the two. Reinstallation of the product and repeats of the tests could not reproduce this odd behaviour, which thus enters the 'unexplained mysteries' file. The misses following the subsequent tests left *KAV* with very close to full detection in all test sets.

NetShield is another product which uses a client-based interface in order to implement changes on the server-based portion of the product. In this case the *NetShield* console is a *Windows*-style application on the client, which attempts to contact the server-based portion of the software whenever it is run and requires a login and server selection on every execution. This requires slightly more rigmarole than the *Kaspersky* control method described above, and requires that the Java runtime environment be present on the client machine before the *NetWare* portion of the product can be installed.

With Java's future on *Microsoft* platforms being uncertain, it remains to be seen what changes will be made to *NAI*'s reliance on the runtime environment in future releases. On a positive note, users familiar with any other *NAI* product will find that the interface here is so similar to that found in others from the same manufacturer that there will be no difficulty in using the *NetWare* software.

The scanning speeds exhibited by *NetShield* were at the slower end of the table, though it was difficult to tell how much of this was due to trans-network interaction since scan speed is often relatively slow for *NAI* products.

Unfortunately *NAI*'s *NetShield* does not become the fifth product to receive a VB100 in this review. Despite having laid to rest the ghost of extension-based misses on most of their platforms, the *NetWare* product failed to detect any of those samples which were extensionless, including one, O97M/Tristate.C, In the Wild. With detection rates elsewhere being close to perfect and no false positives, the misses of these samples may leave a particularly nasty taste in *NAI*'s corporate maw.

NAI McAfee NetShield 4.60 4.160 4.0.4210

ItW File	99.96%	Macro	99.97%
ItW File (o/a)	99.96%	Macro (o/a)	100.00%
Standard	99.88%	Polymorphic	99.92%

Norman FireBreak 4.10.2047 5.00.42

ItW File	100.00%	Macro	100.00%
ItW File (o/a)	100.00%	Macro (o/a)	100.00%
Standard	99.32%	Polymorphic	91.25%

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time(s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	Time(s)	Throughput (MB/s)
CA Vet Anti-Virus	140	3906.7		11	7212.2		86	1853.7	11	6782.5
DialogueScience DrWeb	165	3314.7	[16]	13	6102.6		73	2183.8	13	5739.0
Eset NOD32	65	8414.3		7	11333.4		22	7246.2	4	18651.9
GeCAD RAV	565	968.0		9	8814.9		85	6434.5	11	7212.2
Kaspersky Anti-Virus	230	2378.0		18	4407.4		136	1172.2	32	2331.5
NAI McAfee NetShield	450	1215.4		27	2938.3		165	966.2	37	2016.4
Norman FireBreak	2040	268.1		10	7933.4		20	7970.8	4	18651.9
Sophos Anti-Virus	146	3746.1		20	3966.7		44	3623.1	10	7460.7
VirusBuster VBShield	279	1960.3	1	98	809.5		133	1198.6	40	1865.2

Norman's *FireBreak* returns to the NWAdmin method of control, though it also offers direct control over the single NLM-based server portion. This proved fortuitous because the NWAdmin portion of the application refused to function properly. The method of control used, therefore, was that of interaction directly with the NLM interface. Control on the server was hindered somewhat by the less than intuitive choice of selection keys (for example F5 to select an object for scanning), which are not mentioned on-screen. The readme files do contain this information, though it is buried sufficiently deeply that a casual reader will be very lucky to spot it.

The primary problem for *FireBreak* came with the scanning of the executable clean set. On these files the scanning rate slowed to a snail's pace, becoming increasingly languorous as the test continued. In the past, slow scanning speeds for *Norman* products have been a result of delaying the scan engine deliberately so as not to overload the server, though on this occasion server load reached 100% for considerable lengths of time. However, the other scan speeds were very good and no false positives were detected.

With full detection rates in the ItW and macro test sets, *Norman FireBreak* qualifies for another VB 100%. Weaknesses in detection were, fairly predictably, centred around the newer polymorphics, W32/Etap, W32/Zmist.D and W32/Fosforo. On a slightly more negative note, in log file parsing it was noted that some portions of the path had had their case converted when displayed in the log file, in addition to alteration of '\' to '/' in path descriptions.

Sophos Anti-Virus remains unique in its method of installation, consisting of only a single NLM. When executed this acts in much the same way as a self-extracting executable, creating directories and the files to fill them.

Updates are managed automatically by placing further releases of the NLM into a specified directory, from where the components are extracted. All the functions of the product are controlled through one main NLM installed in this process.

Traditionally, *Sophos* products have been set up with the scanning of compressed files turned off by default, so it came as a surprise to note that the opposite was true in this product. This brings *SAV* in line with most other products in this review, though sadly it also shares with most of those products the lack of a means to browse to targets. Another feature in common with several other products in the review is *SAV*'s habit of mangling log file entries – in this case the crimes were addition of entries for some worms, conversion to 8+3 format and conversion of '\' to '/'.

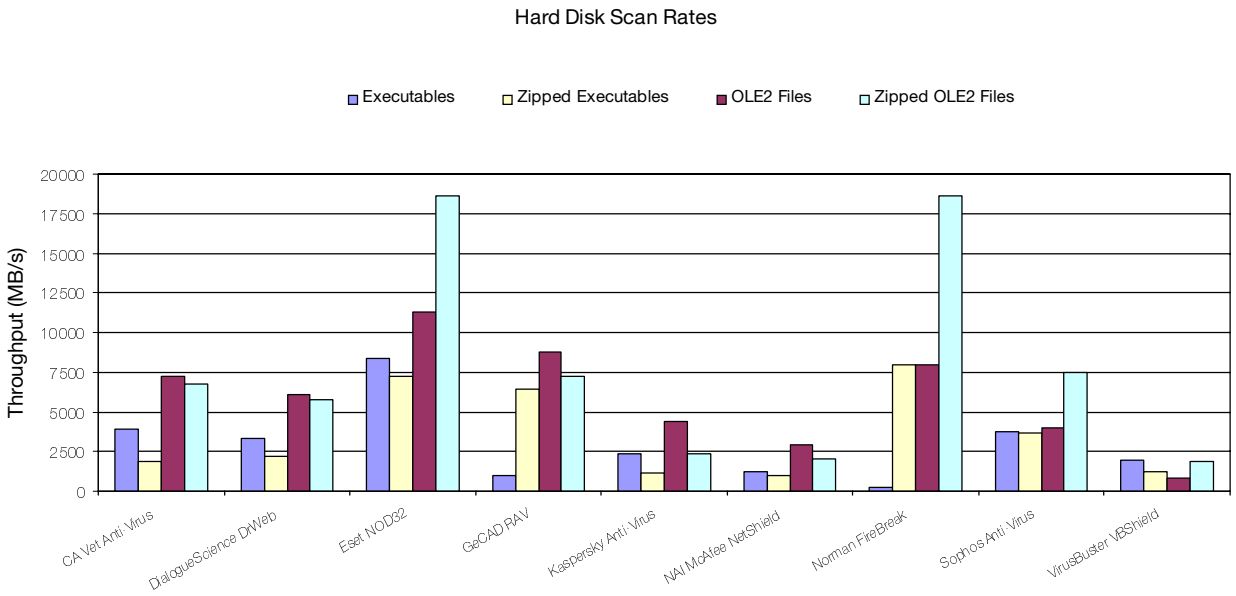
Despite these complaints (which are, by and large, directable towards the majority of the products on offer), *Sophos AntiVirus* performed speedily and with good detection rates. As usual, the samples in the test set that are potentially slow to scan were undetected by choice. This includes the various Access viruses present in the set, mid-infectors such as Positron and DLL-based threats such as Navrhar. Since none of these reside in the ItW set, however, *Sophos Anti-Virus* earns another VB 100 % award.

Sophos Anti-Virus 3.59

ItW File	100.00%	Macro	99.77%
ItW File (o/a)	100.00%	Macro (o/a)	99.67%
Standard	99.43%	Polymorphic	93.31%

VirusBuster VBShield v 1.14.000 7.456

ItW File	99.95%	Macro	100.00%
ItW File (o/a)	99.95%	Macro (o/a)	100.00%
Standard	99.56%	Polymorphic	86.87%



In the previous two *NetWare* reviews, *VBShield* was notable for the fact that its on-demand log files were unusable. It seems that some things never change since this was the case once again, making it necessary for results to be gained by deletion of infected files. Other products featured unusable log files on access, but *VirusBuster* was the only product to do so on demand. Since the problem is simply that the log file splits reports for one file arbitrarily over more than one line if they are over a certain number of characters, this would seem to be an easy and worthwhile fix to implement.

In the previous *NetWare* review, *VirusBuster*'s product suffered the majority of its problems with the polymorphic viruses. This was the case again. Almost all misses for *VBShield* were in the polymorphic test sets, with one of the polymorphic W32/CTX samples being missed in the ItW test set. This was sufficient to deny *VBShield* a VB 100 % award. There were a large number of misses not only amongst the newer but also amonst some of the older polymorphic files. Happily, the comment made in the last review that a significant improvement in detection rates had been seen in *VirusBuster*'s products over the preceding year, can be repeated, although this may make the narrow miss of a VB 100 % all the more disappointing for *VirusBuster*'s developers.

Conclusions

The review finishes on a product for which the comments made in last year's review still ring true, but what is surprising is that the rest of the products reviewed show fewer similarities with their previous incarnations and that my general dislike of *NetWare* has been somewhat mollified over the course of this latest comparative.

In general, the detection rates and ease of use of the products have improved rather more than I dared to hope at the end of the last *NetWare* review. With poorly chosen extension listings for *NAI*, one false positive for *GeCAD* and one missed sample for *VirusBuster* being the three factors preventing a clean sweep of VB 100% awards, this is among the more impressive comparative reviews in terms of product performance. This is deserving of congratulations to all concerned – though tempered with the knowledge that some of the results were let down by such small failings.

NetWare 6 is clearly *Novell*'s customer product of choice at the moment. It is somewhat disturbing that so many companies do not yet have enough confidence in their products on *NetWare 6* to submit them for testing – or have no current product that is usable on *NetWare 6*.

That the market for *NetWare* has suffered considerably during the last half-decade is undeniable, yet the installed user base remains as a market. One feels that, while some companies are active in their development of new features and management tools on *NetWare*, a number of others consider it to be an unpleasant chore to update.

For my prediction I will state boldly that this will not be the year of the *NetWare* virus. With the anti-virus developers reluctant to support *NetWare* when being paid for their expertise, what hope for inspiring virus writers to produce malware for such an operating system? With this thought in mind, *NetWare* looks more appetizing at every turn.

Technical Details

Test environment: Server: 1.6 GHz Intel Pentium 4 workstation with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, running *NetWare 6 Service Pack 1*.

Workstation: 1.6 GHz Intel Pentium 4 workstation with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, l running *Windows NT 4 Service Pack 6*.

Network: 100 Mbit ethernet.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2002/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.