COMPARATIVE REVIEW

NETWARE

Matt Ham

Having set a yearly schedule for comparative testing [*see http://www.virusbtn.com/vb100/about/schedule.xml for the list of forthcoming comparative reviews - Ed*], *Virus Bulletin*'s revisit to *NetWare* this month should not come as a great surprise.

True to form, *Novell* has been busy updating its server software with yet another batch of upgrades and patches. In fact, a new patch was released on the date of finalising the test platform. However, the patch had not been uploaded to *Novell*'s website by midday GMT and therefore it was not included in this test. I suspect that a sigh of relief would have accompanied this decision as far as the submitting anti-virus developers were concerned. Even so, the patch that was used – service pack 1.1 – was a hefty 400 MB addition on top of the server installation. *Novell*'s patches have always been large, but recent patches seem to have set a disturbing trend of exponential increases in size. I await with trepidation the patch required for next year's *NetWare* review.

The line-up for this year's test was similar to that of last year's *NetWare* comparative (see *VB* August 2003, p.17), with *CAT*'s *Quick Heal* the only newcomer to the process. *NetWare* products are very much slower to be upgraded than the operating system upon which they run – leading to a general impression of them as being clunky, irritating and tending towards the user-friendliness of *NetWare 3*. Of course there are exceptions, where the products make use of the multiple methods supplied by *Novell* for integration within ConsoleOne and other admin interfaces. Some companies seem rather indecisive as to which of these paths to pursue and spread control over both. Others use Java or custom GUIs to facilitate administration from clients.

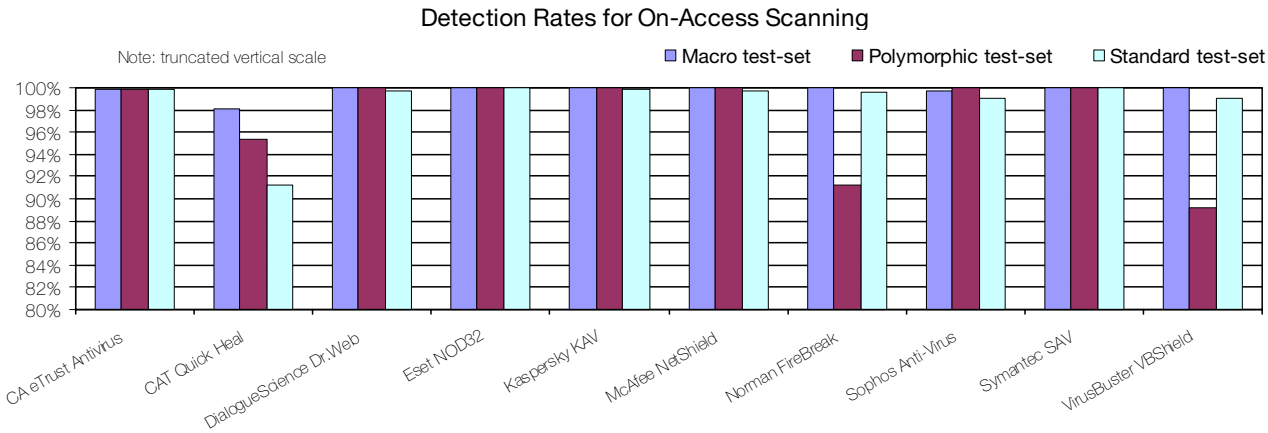
It is remarkable, given the presence of so many ways of accessing scanner functionality over so few products, that the old-fashioned methods are still the most memorable. Problems that have previously been encountered (repeatedly) for products on this platform were noted for inspection once again – it is the presence of so many recurring problems that, perhaps, explains the memories of aged interfaces behaving in unpleasant ways.

TEST SETS

The test sets were aligned with the most recent Real-Time WildList (RTWL: http://www.wildlist.org/WildList/Real-Time.htm) available two days before the submission deadline for products. Since the maintainer of the WildList was on a scheduled vacation at this time, the most recent RTWL was not particularly new. The batch of additions to the test set this month was nowhere near as gigantic as the additions made for the last comparative review (see *VB*, June 2004 p.12) and contained no new samples of any great interest. Given that the newest inclusions were all samples with well-known extensions, and the majority were worms of some sort, it was not anticipated that any of these would cause problems.

One point of note concerning testing is that both on-access and on-demand scans are performed for files located on the server. However, the accesses in the on-access tests are performed from a client machine. Thus there is an additional variable for the throughput functionality when scanning on access – namely that of data transfer from server. Since, in all cases, scanning occurs on the server, the bulk of the information transferred relates to the status of files as being infected or not – which may or may not be transferred to the client directly.

Some products provided popup warnings on the client, and others kept a real-time summary of files scanned and



On-access tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust Antivirus	0	100.00%	12	99.82%	2	99.87%	2	99.90%
CAT Quick Heal	1	99.95%	77	98.13%	882	95.37%	191	91.29%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	3	99.69%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Kaspersky KAV	0	100.00%	0	100.00%	0	100.00%	3	99.85%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman FireBreak	0	100.00%	2	99.95%	180	91.24%	11	99.63%
Sophos Anti-Virus	0	100.00%	11	99.73%	0	100.00%	17	99.09%
Symantec SAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%
VirusBuster VBShield	0	100.00%	0	100.00%	602	89.12%	17	99.01%

infected. However, the level of information in these real-time views seemed to have been reduced considerably in some cases, with the result of lessening network traffic and improving scanning speeds.

CA eTrust Antivirus 7.1

ItW File	100.00%	**Macro**	99.82%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.82%
Standard	99.90%	**Polymorphic**	99.87%

Computer Associates (*CA*) produces new product versions in rapid succession these days – the 7.1 version of *eTrust* coming hot on the heels of version 7.0.

The installation of *CA*'s *NetWare* product is nicely automated, following which the customary patches are applied and licence agreements accepted. The major new development with the product is that the default engine used in scanning is now the *Vet* engine rather than the *CA* engine (a fact which will explain the lack of a dedicated *Vet* product in the comparative review this month).

When initiated from the console the scanning process is very much invisible in terms of what the engine is scanning and whether infections have been found. With options set to log files only, all that results is a counter incrementing in 100-file chunks, reporting scan progress. Only when scanning has completed are infected files noted.

On-access scanning appeared to have no controls whatsoever from within the console, though it did very infrequently send messages to note infected files and it blocked access to most of the infected files offered. Scanning also seemed fairly sluggish and path selection did not offer any browsing to new scan paths or memory of past scan paths. Despite these niggles, however, detection was perfect in the In the Wild (ItW) test set and no false positives were generated in a scan of the clean test sets. The engine-swapped version of *eTrust* thus obtains a VB 100% award.

CAT Quick Heal Antivirus 7.01

ItW File	100.00%	**Macro**	98.13%
ItW File (o/a)	99.95%	**Macro (o/a)**	98.13%
Standard	91.60%	**Polymorphic**	95.37%

The most tricky part of *Quick Heal*'s operation turned out to be the installation. By default this requires access to an ADMIN user with full rights – this user being, from my memory, a throwback to some ancient version of *NetWare*. However, instead of creating an extra user it was possible to bypass the installation application and place the program files directly on the server.

Once the product had been installed scanning looked very fast indeed. The scanner itself was of the old-style console interface – such a lack of modernity had already been hinted at by the installation program, which was a DOS application.

Despite good detection rates in the wild, one missed sample in the ItW test set, together with one false positive in the clean set were sufficient to deny *Quick Heal* a VB 100% by the smallest of margins.

DialogueScience Dr.Web 4.31c

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

Dr.Web remains in the same format as for the last few reviews – that of the traditional-style NLM interface. The interface even retains its green-on-black colour scheme, which will bring back memories (fond or otherwise) to many administrators.

The point of peculiarity of this product is that on-demand scans can be instigated only as scheduled jobs – there is no provision for simply selecting an area and scanning it. *Dr.Web*'s detection rates were certainly high, meaning that it easily achieved a VB 100% award.

ESET NOD32 1.804

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

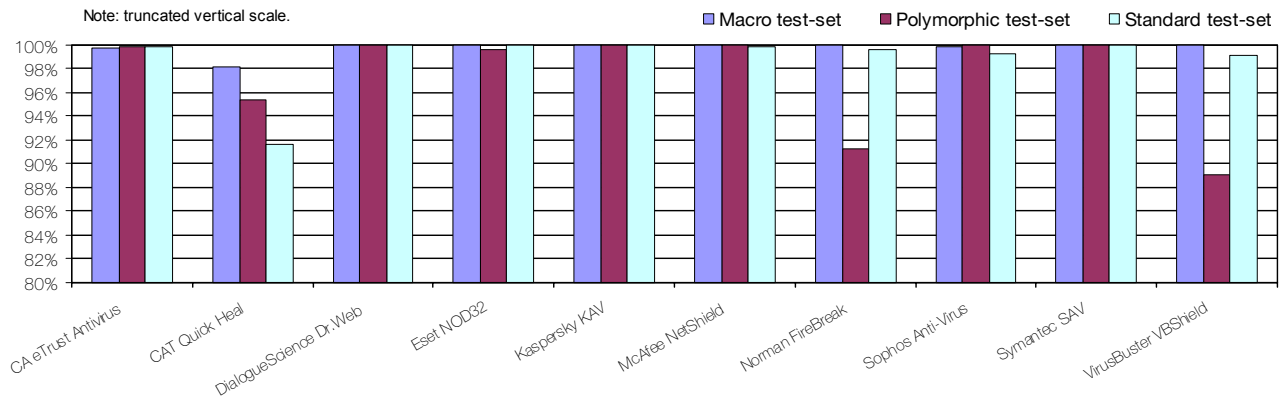
NOD32 for *NetWare* retains the distinction of functioning as two NLMs (a module each for the on-access scanner and on-demand scanner). On-demand scans are performed via a command-line interface. The product has had this configuration for as long as I can remember and, despite being archaic in nature, it serves well as a local solution on *NetWare*. However, external administration options are not the order of the day here – such would have to be created by the user. Despite the antiquated feel of the scanner, detection rates were as might be expected from *NOD32* (given its recent history in *VB* comparatives), with all samples detected both on access and on demand. Since no false positives were noted, *NOD32* is left with a new VB 100% award to add to its collection.

Kaspersky AntiVirus 5.02

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

Yet again, *Kaspersky* has tweaked and changed its method of interface – something which I found rather confusing initially. The hardest part in practice was discovering where, exactly, in the ConsoleOne view a scan is started. The process of setting tasks is carried out through ConsoleOne in a different area, which led to this

Detection Rates for On-Demand Scanning



On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%
CA eTrust Antivirus	0	100.00%	12	99.82%	2	99.87%	2	99.90%
CAT Quick Heal	0	100.00%	77	98.13%	882	95.37%	188	91.60%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	133	99.58%	0	100.00%
Kaspersky KAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee NetShield	0	100.00%	0	100.00%	0	100.00%	1	99.91%
Norman FireBreak	0	100.00%	2	99.95%	180	91.24%	11	99.63%
Sophos Anti-Virus	0	100.00%	3	99.93%	0	100.00%	14	99.24%
Symantec SAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%
VirusBuster VBShield	0	100.00%	0	100.00%	602	89.12%	16	99.19%

momentary confusion. However, once the two areas in which scans are controlled and initiated had been noted, the process became second nature.

Although different from its *Windows* GUI, the GUI provided in *KAV* was a welcome respite from the usual *NetWare* interface, offering a full range of configuration options and, more importantly, not necessitating the typing of long paths when scanning was required. It is of note that the GUI is the only method of scanning control here, Alt-Esc may be used to view the *KAV* console, but no interaction is possible. Scanning on access from a client was considerably faster than using the totally server-based ConsoleOne on-demand scanner. *KAV* landed itself a VB 100% award, its competence lying not merely in its ease of use.

McAfee NetShield 4.62

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.91%	**Polymorphic**	100.00%

For installation of the *NetShield* application to a server, the Java run-time environment must be available – this was a minor irritation since, by default, it was not available on the test clients. Once this has been installed the server can be loaded with the *NetWare* module. In order to interact with this, however, the console software must also be installed on the client machine.

With this completed, the scanner can be used – its look and feel is identical to that encountered with other *NetShield* products. In the past, *NetShield*'s scanning was infuriatingly slow due to excessive communication between the client and server-side portions of the server. By and large, this problem seems to have been remedied in this version of the product. Scanning is still somewhat slow on infected files, though this is a more general feature of the product over multiple platforms rather than being specific to *NetWare*.

Norman FireBreak 4.70.2282

ItW File	100.00%	**Macro**	99.95%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.95%
Standard	99.63%	**Polymorphic**	91.24%

Norman offers interaction with the scanner both through

ConsoleOne snap-ins and the traditional earlier *NetWare*-style interface. The latter was used in this case, since it allows browsing to scan targets and offers no real disadvantages when compared with the more aesthetic GUI.

The same problems were encountered with this product as in last year's *NetWare* review when examining files on access: files are not necessarily scanned if opened only for reading and thus the test set was xcopied with the scanner set to purge any infected files. This worked well, though files were not purged if the read-only flag was set on them – quite an oversight. On-access scanning in this fashion was not particularly fast, even though the heuristics of Sandbox are disabled here by default. Speed is not everything of course, and with *FireBreak* showing full detection of samples In the Wild, and having generated no false positives on a scan of the clean test set, the *Norman* product achieves a VB 100% award.

Sophos Anti-Virus 3.83

ItW File	100.00%	**Macro**	99.93%
ItW File (o/a)	100.00%	**Macro (o/a)**	99.73%
Standard	99.24%	**Polymorphic**	100.00%

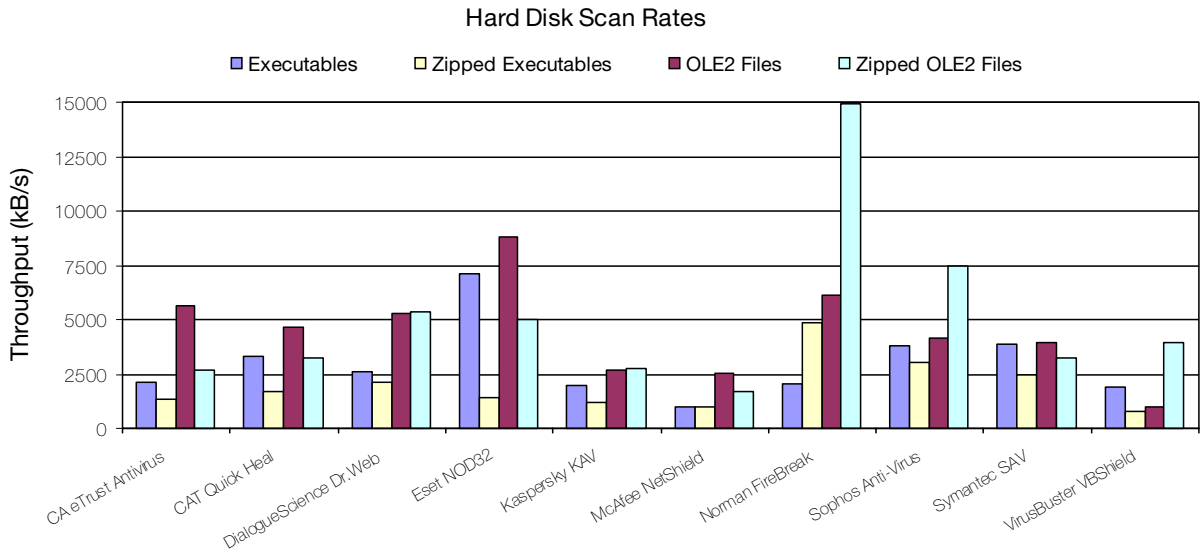
The user interface for *Sophos*'s *NetWare* product has always been something of an abomination, and this is certainly an area where four or so years might have been expected to bring improvements of some sort. My expectations were dashed, however, as the product proved about as user-friendly as a double-ended chainsaw. When scanning it is still necessary to prepend a '>' symbol to paths for recursion, it is still necessary to type each path to be scanned manually, and it is still necessary to append exact file names or wildcards to persuade the product to scan anything at all. Since paths cannot be saved without using them for scanning on every subsequent occasion, it is incredibly frustrating to scan more than one individual target.

On-access scanning is also quirky: all on-access functions are disabled by default and, when enabled, scan only files which are written to the server. Assuming that users may wish to be protected from downloading infected material from their servers, this situation can hardly be considered ideal. The one area in which *SAV* did prove that changes are being made, was detection. Several *Access* files were detected for the first time on demand, and with In the Wild detection complete, a VB 100% award is awarded to the product.

Symantec AntiVirus Corporate 9.0

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

Symantec AntiVirus (*SAV*) is another product which offers control both through a client side application and the server console. The server console controls are extremely limited, however, and the *Symantec System Center* must be installed if anything but the most basic control is to be exerted. This requirement for *SSC* in turn requires certain levels of *Internet Explorer* and *Microsoft Management Console* to be installed on an administrative



Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (kB/s)	FPs [susp]	Time(s)	Throughput (kB/s)	FPs [susp]	Time (s)	Throughput (kB/s)	Time(s)	Throughput (kB/s)
CA eTrust Antivirus	260	2103.6		14	5666.7		120	1328.5	28	2664.6
CAT Quick Heal	165	3314.7	1	17	4666.7		95	1678.1	23	3243.8
DialogueScience Dr.Web	208	2629.5		15	5288.9		75	2125.6	14	5329.1
Eset NOD32	77	7103.0		9	8814.9		112	1423.4	15	4973.8
Kaspersky KAV	278	1967.4		30	2644.5		130	1226.3	27	2763.2
McAfee NetShield	550	994.4		31	2559.2		160	996.4	45	1657.9
Norman FireBreak	272	2010.8		13	6102.6		33	4830.8	5	14921.5
Sophos Anti-Virus	143	3824.7		19	4175.5		53	3007.9	10	7460.7
Symantec SAV	140	3906.7		20	3966.7		65	2452.6	23	3243.8
VirusBuster VBShield	290	1886.0		83	955.8		197	809.2	19	3926.7

machine. Since these are clearly not capabilities offered by *NetWare*, the machine cannot be the server where *NetWare* is installed. Once the rigmarole of the installation procedure was over, however, the product demonstrated few problems and the interface was the standard *Symantec* look and feel – easy enough to obtain when using a central administration tool. Also similar to other *Symantec* products, the detection rates were perfect over all sets, earning *SAV* a VB 100%.

VirusBuster VBShield 1.21

ItW File	100.00%	**Macro**	100.00%
ItW File (o/a)	100.00%	**Macro (o/a)**	100.00%
Standard	99.19%	**Polymorphic**	89.12%

On this occasion the *VirusBuster* product arrived with documentation in a PDF which was unreadable. However, this did not prove to be a major issue, since the installation was identical to that performed for last year's *NetWare* review.

The on-access functions of the product proved easy to find, though on-demand scanning took slightly longer to fathom. On-demand scans must first be assigned as a 'domain' for scanning (which is also where on-access scanning for that area is configured) then scanned as an 'option' in a different area of the interface. Where detection was concerned, matters progressed well, with a VB 100% duly awarded for the product's performance across the ItW and the clean test sets.

CONCLUSIONS

There are good and bad points to be discussed at the end of this comparative. High detection rates and an overall lack of false positives are both gratifying to observe. However, with the increased proportion of simple-to-detect worms in the ItW test set, this was not such an awesome achievement as it might have seemed in the past.

As far as reporting the iniquities of *NetWare* products is concerned, it seems that I am doomed in the same way as Sisyphus to repeat my toils forever to no avail. A brave minority have continued to add new functionality to their products in a pleasant way. However, the products which have irked me in the past through poor design or a desire to become living fossils continue to enrage me. At least I can console myself that I have not paid for such unpalatable software – though I do wonder what customers must think when presented with some of the outrageous anachronisms perpetrated by developers of *NetWare* software.

Technical details

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive. Server running Novell NetWare 6.5 service pack 1.1. Clients running NetWare Client 4.9 service pack 2.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/NetWare/2004/test_sets.html.

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

CORRECTION

VB regrets that an error slipped through the editorial net in the August 2004 *NetWare* comparative review (see *VB*, August 2004, p.14). Despite appearances both in the table for on-demand scanning results and in the results listed in the text, *Eset*'s *NOD32* did not, in fact, miss any samples in the polymorphic test sets. The figure should have indicated an unblemished 100.00%. *VB* apologises for the misinformation.