## COMPARATIVE REVIEW

# NetWare You Wanted to Go?

It is now sixteen months since *Virus Bulletin* published its last *NetWare* comparative review. The hope was that the much-anticipated release of *NetWare 5.0* would have happened in time for this to be *VB's* first review based on that platform. Unfortunately, as seems to be common with major operating system upgrades, the *NetWare 5.0* release has been further delayed. The product submission deadlines could not be however, so, in late April, eleven developers shipped their current *NetWare* server offerings to our Abingdon office.

This number is down somewhat on the previous *NetWare* comparative. Several vendors indicated they were close to releasing 'much improved' versions for this platform (or, more specifically, for *NetWare 5.0*) and would prefer not to have their current versions tested.

### Testing Procedures

Apart from the 'standard' tests of on-demand detection, where the scanner is pointed at the combined test-sets and allowed to run, on-access or real-time detection rates were also measured. This was achieved by running a utility from a workstation that recursed the test-set directory tree, attempting to open every file encountered along the way. For this test, the scanners were configured for on-access detection, as the test utility only tries to open, not write to, the files. (Full 'on-access' scanning is the default setting for very few realtime scanners. For performance reasons just 'on write' or 'on modify' settings are more typical, and for most production systems quite sufficient).

With the increasing dependence upon on-access scanning, a high detection rate alone may not be enough. A product whose on-access component imposes a heavy performance hit on a server will not be highly sought after. Thus, an effort was made to measure the overhead of the various on-access scanning options.

This was achieved by timing how long it took to copy 49 EXE files (all those from SYS:PUBLIC) from one server directory to another. The *NetWare* NCOPY utility was used as it keeps the transfers internal to the server, significantly reducing variations inherent in network transfers. Following a baseline condition, in which the test was run just after a server restart and with none of the scanner components loaded on the server at all, each of the available options and combinations were tested. Each test condition was repeated ten times and the average is reported.

Disk caching can affect the results of such tests dramatically. To reduce such effects in these tests, two runs, whose times were not recorded, were made immediately before each set of ten tests was run. In addition, under baseline conditions one complete test cycle was made and the results discarded before running the actual baseline test.

It seems that many users rely too heavily upon on-demand scanning (at start-up on workstations and scheduled on workstations and servers). Thus, it is with some reservation that the results of the following tests are reported, lest their inclusion should in any way unduly strengthen the perception that on-demand scanning is significantly important.

To measure the speed of the on-demand scanners, the *Virus Bulletin* Clean test-set was copied to a directory on the server and a 'manual' scan run and timed. To nullify any spurious caching effects (which should be small on a 5500 file, 520 MB test-set anyway), the server was downed and restarted immediately before running these tests.

All timed tests (speed and overhead) were run with just the server and one workstation connected via a hub. The workstation was logged into the server as the *NetWare* Admin user. 'Remote' administration programs were not run during any of the speed tests. However, as these were often the only method of changing the realtime scanning settings for the overhead tests, such programs were run at the connected workstation between test conditions, then shut down while the tests ran. The overheads are presented in percentage terms in the results table and normalized to a ten second baseline in the graph of overhead results.

In general, the suggested installation defaults were accepted. Two exceptions were made to this – offers to scan the server during or straight after setup, and requests to modify the server's AUTOEXEC.NCF file, were declined.

### Test Sets

The 'usual' *Virus Bulletin* test-sets were employed, with the exception of the In the Wild Boot set, as boot infector scanning is not directly relevant to NLM-based products. The BIOS and DOS routines 'underlying' *NetWare* are completely cut off once the server loads, so any viruses present there will not affect the server (unless they corrupt something during the machine bootstrap or server load phases). Some products offer the option of scanning the DOS memory of the server anyway, providing a chance to raise a warning should there be something of concern run during your server boot process.

This does not mean that *NetWare* servers are 'immune' to boot viruses – we hear too many tales of woe about infected diskettes and/or long-term infections of some payload-toting virus where the affected server happens to be rebooted one too many times or on the 'wrong' date. Avoiding these kinds of problems, or even warning you of them, is not something a *NetWare*-hosted scanner can

| On-demand tests | ItW File | | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | Number | % | Number | % |
| **CA Cheyenne Inoculan** | 666 | 100.0% | 1085 | 93.0% | 13489 | 99.0% | 921 | 100.0% |
| **Command AntiVirus** | 666 | 100.0% | 1162 | 99.3% | 13499 | 99.1% | 921 | 100.0% |
| **Cybec Vet NetWare** | 658 | 99.4% | 1114 | 95.4% | 13498 | 99.1% | 916 | 99.4% |
| **Data Fellows FSAVN** | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 921 | 100.0% |
| **Dr Solomon's AVTKN** | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 921 | 100.0% |
| **Intel LANDesk Virus Protect** | 666 | 100.0% | 1146 | 98.0% | 13500 | 100.0% | 921 | 100.0% |
| **Kaspersky Lab AVPN** | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 921 | 100.0% |
| **Norman FireBreak** | 666 | 100.0% | 1132 | 96.8% | 13495 | 99.0% | 921 | 100.0% |
| **Sophos SWEEP** | 666 | 100.0% | 1158 | 99.0% | 13500 | 100.0% | 917 | 99.4% |
| **Symantec Norton AntiVirus** | 666 | 100.0% | 1142 | 97.7% | 13500 | 100.0% | 921 | 100.0% |
| **Trend Micro ServerProtect** | 623 | 91.9% | 902 | 77.2% | 12411 | 90.2% | 881 | 96.5% |

reliably do. The long and short of this is that these scanners are not run against the In the Wild Boot test-set, so the *VB 100%* awards are based solely on results against the In the Wild File test-set.

The other interesting thing to note is that, since the last review, the Macro test-set has been augmented with samples of the first *Microsoft Access 97* macro viruses. A few vendors were claiming detection of these within days of their appearance in mid-March, so it will be interesting to see how many had built this capability into the product they were shipping in late April.

So, how did the eleven products stack up? Let's find out...

## CA Cheyenne Inoculan v4.0

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 93.0% |
| ItW File on-access | 100.0% | Macro on-access | 93.0% |
| Standard | 100.0% | Polymorphic | 99.0% |

Following initial problems with installing the product because a licence key was not provided with the review copy, proceedings picked up greatly. *Inoculan* displayed some admirable detection gains over recent *Virus Bulletin* test results, particularly against the Polymorphic and In the Wild File test-sets, attaining its first VB 100% award for the latter performance. On the Macro test-set, 93.0% is a little disappointing, and somewhat surprisingly it was mainly *Word 7* viruses that caused *Inoculan* trouble.

The *Inoculan* approach to anti-virus issues is to provide tools for the centralized management of server scanning and workstation deployment and management. To this end an administration program is run from a workstation to configure and monitor the server-based scanner.

Although replete with configuration options, several 'features' of the user interface of the management program are truly irksome. Spin-dials are great interface gadgets for the mouse-bound, and are normally quite tolerable to keyboarders. However, when you cannot type entries into them – particularly when the intention is to maximize the log file size from its default of 100 lines to its upper limit of 32,767 – they rapidly become a major annoyance. All the spin-dials in *Inoculan* need to be fixed! A quick search for the file holding the log file configuration options and some trial-and-error editing saw this 'problem' resolved in time to make the review copy deadline.

A configuration option involving special handling of certain server I/O calls, including those generated by NCOPY, caused some problems in the overhead tests. The product worked fine, but reliable timing data could not be recorded

| On-access tests | ItW File | | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | Number | % | Number | % |
| CA Cheyenne Inoculan | 666 | 100.0% | 1085 | 93.0% | 13489 | 99.0% | 921 | 100.0% |
| Command AntiVirus | 666 | 100.0% | 1162 | 99.3% | 13499 | 99.1% | 921 | 100.0% |
| Cybec Vet NetWare | 658 | 99.4% | 1114 | 95.4% | 13498 | 99.1% | 915 | 99.3% |
| Data Fellows FSAVN | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 919 | 99.7% |
| Dr Solomon's AVTKN | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 921 | 100.0% |
| Intel LANDesk Virus Protect | 666 | 100.0% | 1146 | 98.0% | 13500 | 100.0% | 921 | 100.0% |
| Kaspersky Lab AVPN | 666 | 100.0% | 1162 | 99.3% | 13500 | 100.0% | 919 | 99.7% |
| Norman FireBreak | 666 | 100.0% | 1132 | 96.8% | 13495 | 99.0% | 921 | 100.0% |
| Sophos SWEEP | 666 | 100.0% | 1158 | 99.0% | 13500 | 100.0% | 917 | 99.4% |
| Symantec Norton AntiVirus | 666 | 100.0% | 1142 | 97.7% | 13500 | 100.0% | 921 | 100.0% |
| Trend Micro ServerProtect | 623 | 91.9% | 902 | 77.2% | 12411 | 90.2% | 881 | 96.5% |

for test conditions that involved intercepting file write operations. Of the five false positives recorded against the Clean test-set, three were for the ‘Texas’ virus.

## Command AntiVirus for NetWare v4.50β

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.3% |
| ItW File on-access | 100.0% | Macro on-access | 99.3% |
| Standard | 100.0% | Polymorphic | 99.1% |

This beta version of *Command AntiVirus for NetWare* (*CSAVN*) sees the long-awaited *F-PROT v3.00* detection engine first come under scrutiny in a *Virus Bulletin* test. The new engine certainly exhibits the much-needed detection improvement that has been promised for so long. Perhaps not surprisingly, there is a particularly noticeable improvement over recent *CSAV* and *Command F-PROT Professional* results in the Polymorphic test-set.

As noted in the recent standalone review of *CSAVN* (see *VB*, March 1998, p.21), the name transition is not complete throughout the product. In some places the name ‘F-PROT’ appears, whereas in others the reference is to ‘CSAV’. This continues through the documentation and on-line help, but will hopefully be corrected by the time this product completes its beta phase.

Installation is performed by the near ubiquitous (in the *Windows* world) *InstallShield*. Server components are copied to SYS:SYSTEM and a *Windows*-based administration program is installed to the workstation.

Across the other products in this review there is an either/or approach to administering the server-based scanner – it is either all done at the server console (and thus can be remotely managed via RCONSOLE) or all done with workstation-based administration tools. Neither is really ‘right’ or best for everyone.

The designers of *CSAVN* acknowledge this by allowing virtually full administration from the server console (by extending the server’s command set with a range of CSAV commands) or from a workstation-based administration program. The only possible addition we could suggest is the inclusion of a scripting capability, though we are prepared to concede that there may in fact be one there already – being a beta, the software still had a few rough edges, but the documentation was lagging well behind!

*CSAVN* was certainly not the fastest product in the round-up, and the overhead imposed by its on-access component was also very high. Being a beta version, it may be too early to make definitive statements about such performance issues, but potential purchasers should check this carefully when the product is released.

| | Overhead | | | | Scanning Speed | | False Positives |
|---|---|---|---|---|---|---|---|
| | Loaded Inactive | Read or Outgoing | Write or Incoming | Read and Write | Time (min:sec) | Throughput (KB/s) | |
| **CA Cheyenne Inoculan** | 25.0% | 35.7% | | | 21:01 | 423.6 | 5 |
| **Command AntiVirus** | 17.1% | 88.4% | 127.5% | 122.1% | 54:49 | 162.4 | 1 |
| **Cybec Vet NetWare** | -1.5% | 33.0% | 28.2% | 29.9% | 9:07 | 976.4 | 12 |
| **Data Fellows FSAVN** | 4.8% | 56.4% | 44.7% | 49.2% | 17:22 | 512.6 | 4 |
| **Dr Solomon's AVTKN** | -2.7% | 109.5% | 71.1% | 147.9% | 39:47 | 223.8 | 0 |
| **Intel LANDesk Virus Protect** | 9.0% | 6.1% | 45.6% | 44.4% | 15:41 | 567.6 | 0 |
| **Kaspersky Lab AVPN** | 4.6% | 46.8% | 34.6% | 43.7% | 17:40 | 503.4 | 4 |
| **Norman FireBreak** | 0.2% | 5.6% | 25.2% | 31.0% | 13:03 | 682.1 | 0 |
| **Sophos SWEEP** | -1.6% | | 34.4% | 89.6% | 12:00 | 741.8 | 0 |
| **Symantec Norton AntiVirus** | 0.7% | 59.4% | 58.5% | 68.3% | 7:01 | 1268.7 | 0 |
| **Trend Micro ServerProtect** | 4.8% | 41.9% | 45.9% | 48.8% | 25:47 | 345.3 | 3 |

## Cybec Vet NetWare v9.70

| | | | |
|---|---|---|---|
| ItW File | 99.4% | Macro | 95.4% |
| ItW File on-access | 99.4% | Macro on-access | 95.4% |
| Standard | 99.4% | Polymorphic | 99.1% |

Since *Virus Bulletin* last reviewed this product it has experienced a name change (see *VB*, October 1997, p.18). The developers have added email and SNMP trap alerting methods. Installation must proceed from a PC running *Windows 95* or *NT*, and looks much like other *Vet* setup routines. An option common to many products in this review is the ability to select multiple servers and concurrently run the same installation or update on all of them.

A twist to this, unique to *Vet*, is that at the end of the setup process you can return to the server selection list and choose another set of servers to receive a different configuration, and so on, avoiding repeating the first part of the setup rigmarole. Apart from this multi-server installation option, there appear to be no facilities for grouping multiple servers into management 'domains' nor for automating updates across or between servers.

Immediate scans default to 'blind' scanning mode, whereas on-access scanning defaults to 'intelligent' mode. This explains why, in the on-access test, *Vet* missed the same viruses as on-demand plus a Midin.765 sample – the 'blind' scanner would run across this mid-infector regardless of where its code ended up in the host, whereas the 'intelligent' scanner would only catch infections where the code happened to fall in an area considered 'important to scan'.

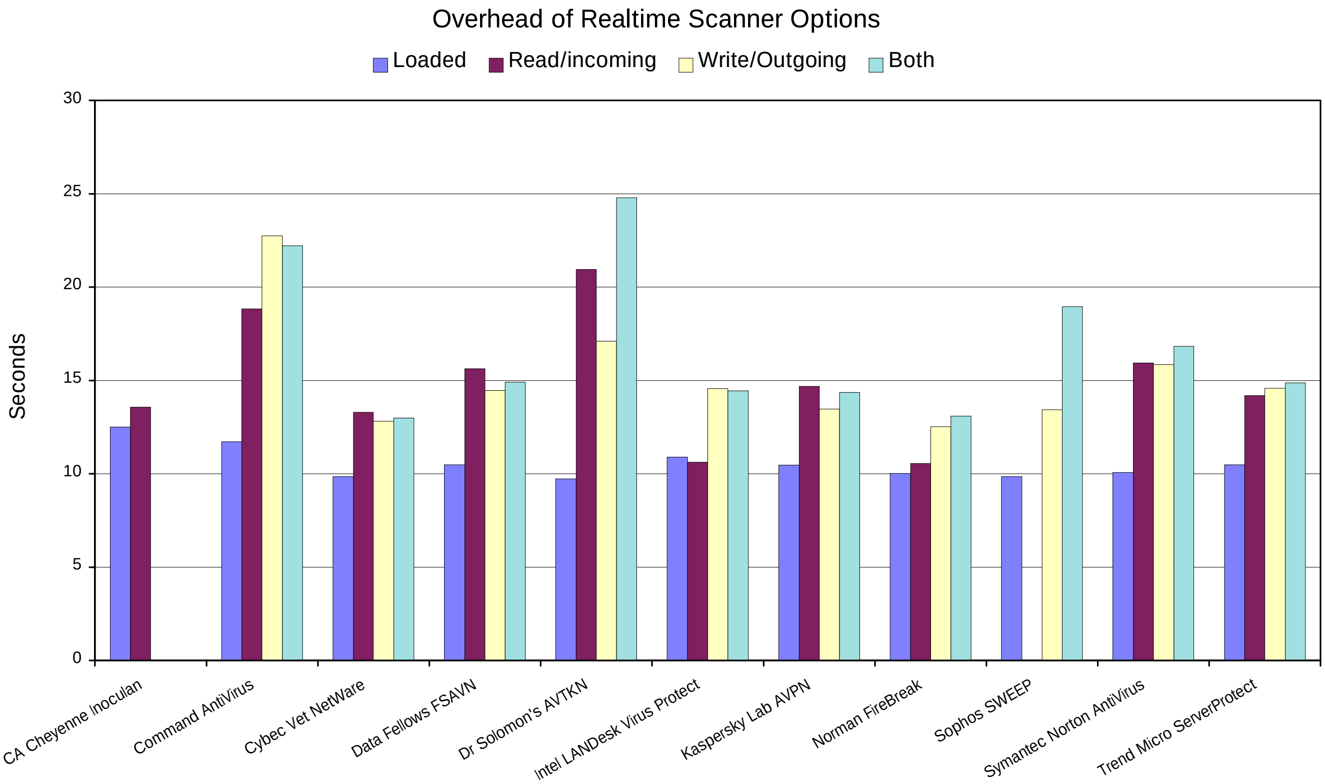
*Vet's* on-demand scanning speed was considerably faster, with a throughput of 2234.8 KB/s, if set to 'intelligent' mode for that test. The false positives were all of the HLLO.40932 virus, suggesting a poorly chosen scan string – the developers claim this is now fixed.

## Data Fellows F-Secure Anti-Virus v4.00

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.3% |
| ItW File on-access | 100.0% | Macro on-access | 99.3% |
| Standard | 100.0% | Polymorphic | 100.0% |

As with their DOS scanner, included in the February 1998 comparative, *Data Fellows' F-Secure for NetWare* (*FSAVN*) uses only one of the two engines the company licenses – *AVP* from *Kaspersky Lab*.

In fact, the product is essentially a re-badged *AVP for NetWare*. A readme file supplied with the product promises a *Windows*-based administration client 'in an upcoming release', but in the meantime you still need a *Windows 95* machine (running *Client32* – *Novell's* 32-bit *NetWare* client for *Windows 95*) to run the installation program. A unique



feature (within this review group) was that at the end of the brief installation process, the scanner was auto-loaded on the server. Beyond this, functionality and performance were identical to *AVP for NetWare*, and the reader is referred to that product's review section for more details.

## Dr Solomon's AVTK for NetWare v7.83

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.3% |
| ItW File on-access | 100.0% | Macro on-access | 99.3% |
| Standard | 100.0% | Polymorphic | 100.0% |

Although still at the head of the pack in terms of virus detection, the rest of *Dr Solomon's Anti-Virus Toolkit for NetWare* (*AVTKN*) seems to be suffering a serious case of arrested development. Compared to *InstallShield*, INSTALL.BAT hardly sets the image of a product for the late 1990s.

The complex and potentially powerful configuration scripts are still present, yet the simple, *Windows*-based configuration editor displays its lack of currency with a message in the Help/About box saying 'Copyright (C) S&S International PLC 1995'.

Worse, there was three-way discrepancy with regard to the on-line help, the printed documentation and the interface of the reviewed product. This was particularly noticeable in configuring the realtime component of *AVTKN*. File Access Monitor v7.83 wishes to disinfect by default, yet this is not even mentioned as an option in the documentation or on-line help. 'Unconfiguring' this option was quite a battle. Nor did the configuration editor hint that an option it did not understand was the preset default. Further, none of the 'intuitive' options that were tried in manual editing of the configuration file worked either. In the end a setting of 'Alert on Reads, Rename on writes' was the nearest setting to the desired 'report only'.

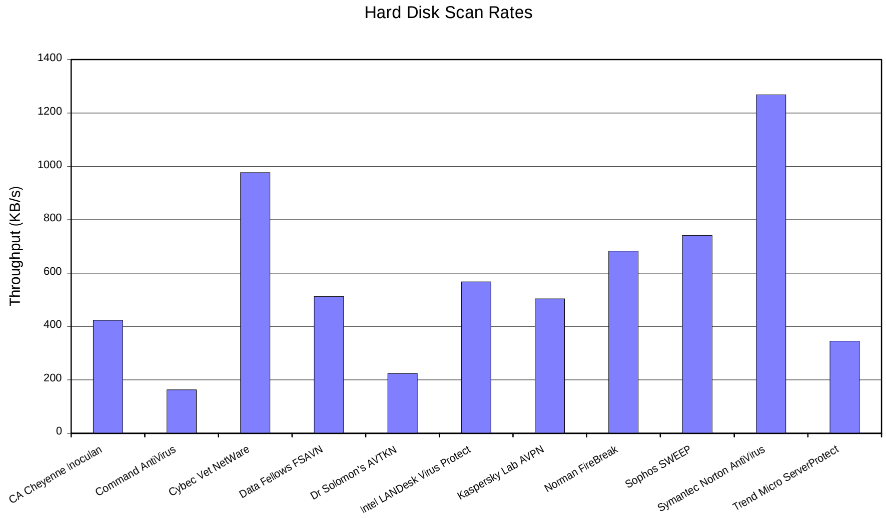
The clunky interface aside, *AVTKN's* detection performance left little to be desired, only missing the four samples of each of the *Access 97* macro viruses. Speed and overhead were not stunning, but *AVTKN*, by default, pauses briefly between files it scans so as not to hog the CPU. This can be disabled for on-demand scanning and doing so resulted in throughput improving to 355.1 KB/s.

## Intel LANDesk Virus Protect v5.02

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 98.0% |
| ItW File on-access | 100.0% | Macro on-access | 98.0% |
| Standard | 100.0% | Polymorphic | 100.0% |

Apart from signature updates, this is the same version of *Intel LANDesk VirusProtect* (*LDVP*) reviewed in the February 1998 issue. Readers are referred to that review for details of *LDVP's* functionality. In brief, this is a full-featured product, from the network manager's perspective, and this version leaves little to be desired from that quarter.

An *LDVP*-protected server can automatically update from another server within your organization or from the Internet (via FTP) or a BBS. Checking these sources for updates can


Hard Disk Scan Rates

be scheduled, although only one source can be configured as 'active'. Domains of like-configured workstations and servers can be controlled centrally. Workstation settings can be 'locked' to prevent fiddling fingers interfering with your corporate anti-virus policy implementation.

A *Windows 95* or *NT* workstation is required for the installation and administration. *LDVP* now incorporates the *IBM* anti-virus engine, perhaps accounting for the significant detection gains evident here.

## Kaspersky Lab AVP for NetWare v3.0

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.3% |
| ItW File on-access | 100.0% | Macro on-access | 99.3% |
| Standard | 100.0% | Polymorphic | 100.0% |

*Kaspersky Lab's* product continues its tradition of high detection rates, albeit at the cost of raw speed. *AVP for NetWare* (*AVPN*) and its *Data Fellows FSAV* incarnation were the only products to detect any of the *Access 97* viruses in these tests, finding all four A97M/AccessiV.A samples.

Another product taking a minimalist approach, *AVPN* is installed through the simple expedient of perusing a readme file then copying the appropriate files to a suitable directory on the server. Should you elect to install *AVPN* in a differently-named folder from the suggested default, a few minor tweaks will need to be made to the supplied NCF loader script, and then it is ready to run.

There are neither network-wide management tools nor mechanisms for distributing signature database updates from one server to another. Although the NLMs do not need to be unloaded from the server to activate signature updates, you must manually activate such updates from a menu. This can be achieved remotely via RCONSOLE.

The default settings for the on-line scanning option include scanning only COM and EXE files. For the purposes of fair testing, this was changed to all files (*.*) – the same as the default for on-demand ('manual') scans. This non-default setting was used for all on-access tests, including those of scanner overhead.

The on-line scanner was overwhelmed by the on-access test procedure. Its report files indicated finding approximately 10% of the total test-set, and most of these detection reports were duplicated in the report files.

After several unsuccessful attempts to cajole *AVPN* into better co-operation, it was configured to delete infected files and the file access process was modified to recurse the test-set directory tree repeatedly, attempting access to each file found there. This was left running overnight and when the scanner was clearly not deleting any more files the test was deemed to have reached completion. Four false positives were reported in the Clean test-set.

## Norman FireBreak v3.86

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 96.8% |
| ItW File on-access | 100.0% | Macro on-access | 96.8% |
| Standard | 100.0% | Polymorphic | 99.0% |

Variously labelled *Norman Virus Control for NetWare* and *Norman FireBreak*, this Norwegian product reaffirms *Norman's* recent record of very good detection performance in *VB* tests.

A *Windows* client PC is required for the installation of *Norman FireBreak*, due to its use of *InstallShield*. Apart from this, the product seemed to be a fairly traditional *NetWare* console application, with no remote administration software or the like. Unloading of the NLM and access to its configuration menu can be password protected, but this option is not set by default. Either way, you cannot unload the NLM from the System Console but only from the *FireBreak Console*.

*FireBreak* can be configured as a 'communications hub'. In a multi-server network, such a hub becomes a central point to which other, suitably configured, *FireBreak*-protected servers can send virus incident reports. Beyond this centralized reporting, logging and alerting capability however, *FireBreak* does not seem to provide for multi-server management or LAN-wide updating. Somewhat confusingly, several of the menus refer to 'manual/scheduled' scanning, but there was no apparent mechanism for configuring scheduled scanning – something of an odd omission in a server product.

Similarly to *Dr Solomon's AVTKN*, *FireBreak* provides a command-line option to remove its inter-file scan delay. This could be handy for speeding up scans when the server is not under a heavy load, such as in the evenings or at weekends before a backup is due to start. Utilizing this option and repeating the throughput test resulted in a slightly better performance of 809.3 KB/s.

## Sophos SWEEP v3.09

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 99.0% |
| ItW File on-access | 100.0% | Macro on-access | 99.0% |
| Standard | 99.4% | Polymorphic | 100.0% |

*SWEEP* has a very simple installation procedure – copy the supplied NLM to the server (preferably to the SYS:SYSTEM directory). You have to do this 'manually'. It seems that the effort of writing an installer to copy just one file has, perhaps unsurprisingly, been deemed not worthwhile by *SWEEP's* developers.

Actually, this comment is a little unfair – on first loading *SWEEP* on the server, it detects that it has not run before and sets itself up. This includes making a 'home' directory for itself, and others in which to 'quarantine' infected files and to manage the server side of its interface to *InterCheck* (should you choose to use this machine as an *InterCheck* server for your workstations). It also installs a number of other files that are packed inside the main NLM.

Since last reviewing this product, some basic update management facilities have been added. *SWEEP* can now be configured to look for an upgraded NLM in a directory on the server, and when one is detected, it will unload itself and load the new one (this process has some integrity checks built into the replacement NLM). There is also a companion NLM allowing 'remote scripting' control of the console command line.

Although claiming NDS awareness, in testing *SWEEP*, it seemed unable to consider objects to scan other than at the volume, directory and file levels. It could be configured to ignore objects at the directory and filename levels, though wildcards are not allowed, potentially limiting its usefulness. The extent of *SWEEP's* NDS awareness appears limited to selecting NDS user groups for alerting purposes.

The scanning speed reported is for *SWEEP's* first run, in which it creates checksums for *InterCheck's* use (whether you use *InterCheck* in client-server mode or not). A subsequent run returned a throughput of 989.1 KB/s.

## Symantec NAV for NetWare v3.xx

| | | | |
|---|---|---|---|
| ItW File | 100.0% | Macro | 97.7% |
| ItW File on-access | 100.0% | Macro on-access | 97.7% |
| Standard | 100.0% | Polymorphic | 100.0% |

*Symantec's Norton AntiVirus* (*NAV*) was yet another product using *InstallShield*, which installed the server scanner and workstation-based administration components. On detecting it was installing to a *NetWare 4.1x* server, the option of adding a *NAV* 'snap-in' to the *NetWare Administrator* program was offered.

Missing the *Access 97*, and a small number of recent *Word 97*, macro viruses, *NAV* continues on its course of improved virus detection.

## Trend Micro ServerProtect v3.51 VPN 362

| | | | |
|---|---|---|---|
| ItW File | 91.9% | Macro | 77.2% |
| ItW File on-access | 91.9% | Macro on-access | 71.2% |
| Standard | 96.5% | Polymorphic | 90.2% |

Another product aiming to be a complete network anti-virus management solution is *Trend's ServerProtect for NetWare* (*SPNW*). It has a graphical installation routine, workstation-based administration and very minimal functionality or configurability at the server console.

Various server and workstation components display copyright notices mentioning *Intel* as well as *Trend Micro*, and the general look and feel of the product suggests something of an older version of *Intel's LANDesk Virus Protect*. Indeed, much of the terminology, and even the default domain protection password, is the same.

Unfortunately, instability in the review copy led to very low detection rates. The patch shipped to fix this resulted in some of the previously detected viruses (including the *Access 97* macro viruses) not being detected. Use of a significantly newer virus signature file improved detection dramatically, but inclusion of those results would unfairly disadvantage the other products in this review.

### Conclusion

As far as feature sets go, the tested products clearly cover a broad range. At one end of the spectrum are the simple single server scanners, controlled from the *NetWare* system console. Apart from detecting viruses, these have little in common with the 'Starship Enterprise' models that allow for a single point of management and update for all servers (often *NetWare* and *NT*) and all common desktop machines within the organization.

It is encouraging to note the continuing improvement in overall detection, although it should be remembered that a somewhat depleted set of products has been tested.

**Technical Details**

**Hardware:** Server – *Compaq Prolinea 590*, 90 MHz Pentium with 80 MB of RAM, 1 GB hard drive, running *NetWare 4.10* with LIBUPG and 410PT8B applied. Workstation – 166 MHz Pentium with 4 GB hard drive and CD-ROM drive, running *Windows 95* with *Novell's Client32*.

**Test Sets:** Complete listings of the test-sets used can be found at http://www.virusbtn.com/Comparatives/NW/199807/test_sets.html. Note that this listing includes the In the Wild Boot test-set although it was not used in this review.