COMPARATIVE REVIEW

Half Full or Half NT?

Starting a *VB* comparative of this size is a sobering prospect, much like beginning Hercules' labours with a tight deadline attached. Three thousand boot sector tests and some three-quarters of a million file tests later, the results are out and begging for analysis.

NT is now a well-established and growing platform, with more advanced versions still a distant prospect. Therefore, it should be expected that the products reviewed were able to take advantage of this stable background, detecting well, and with the minimum of glitches.

As ever this turned out not to be the case, and it was not just the new versions causing aggravation or frustration with their ability to lock the test machines. Who were the dismal failures hanging their heads in shame, and who the virus-vanquishing heroes? Read on.

Test Procedures

The platform used for these tests was *NT 4.0* with service pack 3. The same machine was used for all time-tests, while two other hardware-identical machines were employed in conjunction for the scanning processes.

In all cases, the software was deployed in its standard configuration, unless this removed such useful features as on-access scanning, and was run from the Administrator usercode. Several products were submitted along with pleas from their developers that default settings not be used, since they did not scan, for example, MDB files, and that 'all files' be used as an option. For fairness' sake, all such pleas were ignored, as several products which would also detect such viruses with their settings changed were not accompanied by similar requests.

The June WildList was used as the basis of the In the Wild test-set. This, in conjunction with the ever-expanding Macro, Polymorphic and Standard *VB* test-sets, was tested against products submitted by the 3 July deadline. Of special note was the addition of Win95/Marburg and four Win95/CIH variants to the set, which is discussed later.

Also of note were the first VxDs to grace the *VB* test-set in the form of Navrhar. Another interesting 'new addition' was WM/Pwd.A, a macro virus which password-protects infected files. Several products were unable to open the files, which was counted as a non-detection, compared to those which were adamant that a virus was present.

Scan tests were run where possible from CD, thus removing the need to restore files after each scan as a precautionary measure against over-keen deletion or disinfection. Several products, however, generated report files that were either useless or nonexistent. In these cases deletion or quarantining were used in order to produce meaningful results.

Timing tests were run on various operations. On-access scanning overhead was tested using XCOPY to move large numbers of executables, the results being compared against a baseline and normalized across the products. Floppy disk speed tests were performed upon two almost identical disks, differing only in that the files on one were universally infected with Natas.4744.

The hard disk scanning test, combining speed and false positive testing on 5500 executables in the *VB* Clean test-set, should produce results directly comparable with results in the last *NT* review.

The complete detection tests are reported in the main tables. The results reported in the summaries are only the on-demand ones, plus the on-access result for the combined In the Wild test-sets, where applicable.

Alwil AVAST32 v7.70

ItW Overall	100.0%	Macro	98.7%
ItW Overall (o/a)	n/t	Polymorphic	94.8%
ItW Boot	100.0%	Standard	98.4%

Commencing with a sound VB 100%-worthy result, *Alwil's* product continues to put in good performances. All cannot, however, be said to be rosy. *AVAST32* is the second slowest of the products tested when faced with the Clean test-set – in the region of half the scanning rate of the next fastest product. This set also caused *AVAST32* to throw up some cryptic error messages, which declared that the files involved were untested due to 'error e100 f125'.

As the first-encountered product in this review, *AVAST32* also sets the precedent of missing A97M/AccessiV, Win95/Marburg, Navrhar and Win95/CIH. Since CIH and Marburg are flavour of the month, these are discussed later in some detail.

In terms of ease of interface use, *Alwil* has done enough to be rated above average, with no tasks causing particular difficulty. The same cannot be said of the on-access detection routines, however. Although present, these are only able to detect viruses upon execution. Since executing samples, rebooting and rebuilding the machine from disk image backups some 17,000 times is a little impractical, the on-access scanner was left untested against the file viruses. On-access detection of ItW Boot set showed the age-old problem of non-detection if faced with boot sectors with 'strange' BPBs. This has been discussed at great length in *VB's* two preceding *NT* comparatives.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil Avast32	88	100.0%	665	100.0%	100.0%	1490	98.7%	13500	94.8%	952	98.4%
CA Cheyenne Inoculan	88	100.0%	665	100.0%	100.0%	1338	90.3%	13489	93.8%	952	98.4%
Command AntiVirus	88	100.0%	665	100.0%	100.0%	1498	99.2%	13494	93.9%	952	98.4%
Cybec Vet AntiVirus	88	100.0%	665	100.0%	100.0%	1441	97.4%	13500	94.8%	947	97.9%
Data Fellows FSAV	88	100.0%	665	100.0%	100.0%	1501	99.5%	14244	100.0%	1006	99.7%
DialogueScience Dr Web	87	98.9%	665	100.0%	99.9%	1465	98.9%	14244	100.0%	1006	99.7%
Dr Solomon's AVTK	87	98.9%	665	100.0%	99.9%	1461	98.7%	13500	94.8%	961	98.7%
EliaShim ViruSafe	87	98.9%	659	99.6%	99.5%	1360	92.9%	13243	91.7%	946	97.9%
ESET NOD32	88	100.0%	665	100.0%	100.0%	1461	98.5%	13813	96.4%	970	98.8%
GeCAD RAV	88	100.0%	656	99.2%	99.3%	1480	99.0%	13483	92.1%	901	93.7%
Grisoft AVG	73	83.0%	663	99.7%	97.7%	1243	83.8%	12996	90.4%	936	97.1%
H+BEDV AntiVirNT	86	97.7%	602	94.6%	95.0%	1419	95.9%	10959	76.1%	940	95.9%
Kaspersky Lab AVP	88	100.0%	665	100.0%	100.0%	1501	99.5%	14244	100.0%	1015	100.0%
NAI NetShield NT	88	100.0%	656	99.4%	99.5%	1446	97.7%	13435	92.7%	945	97.9%
Norman TBAV	88	100.0%	665	100.0%	100.0%	1447	97.7%	13496	93.0%	981	98.9%
Norman Virus Control	88	100.0%	665	100.0%	100.0%	1435	96.8%	13498	93.9%	973	97.1%
Proland Protector Plus	25	28.4%	307	49.8%	47.3%	589	39.1%	1465	9.5%	257	36.1%
Sophos SWEEP	88	100.0%	665	100.0%	100.0%	1454	98.2%	13810	96.4%	959	98.3%
Symantec Norton AntiVirus	88	100.0%	665	100.0%	100.0%	1417	95.8%	13500	94.8%	952	98.4%

CA Cheyenne Inoculan v4.00

ItW Overall	100.0%	Macro	90.3%
ItW Overall (o/a)	94.9%	Polymorphic	93.8%
ItW Boot	100.0%	Standard	98.4%

While the general trend in products reviewed seems to be of gradual improvement, *Computer Associates* (*CA*) has seen fit to continue flying in the face of fashion. Scanning the Clean test-set, *Inoculan* continued its unenviable record of causing access violations, crashing *NT* when faced with the unarchiving utility unp.exe. Not overly fast when this program was removed, floppy disk scan speeds were also somewhat greater than the mean, while overhead for the resident portion of the program was average. Having said that, the 'average' overhead seen in these tests was something in the order of 100% – doubling the time taken to copy files, and most certainly a painful side effect.

On-demand scanning proved uncharacteristically quick and easy for boot disks, yet astonishingly slow for the file viruses. Log files were impossible to obtain, since printing results to a file resulted in lines garbled by *Inoculan's* cunning use of linefeeds and pagebreaks.

On-access, the boot sector scanner sent *NT* into blue-screened apoplexy on several occasions – it mattered little whether the disk proffered was infected or not. The on-access scanner was still unable to penetrate the mystery of strange boot sectors.

Despite this, *CA's* product managed to gain a VB 100% award and reasonable, if not notable, detection in other areas. To carry on with this tester's metaphor – it is likely that the *Inoculan* user will compare it to the shirt of Nessus, as worn by Hercules in his later days. It certainly offers some degree of protection but the agony involved in using it is out of all proportion to its utility.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
CA Cheyenne Inoculan	75	85.2%	664	99.9%	94.9%	1338	90.3%	13489	93.8%	952	98.4%
Command AntiVirus	75	85.2%	665	100.0%	94.9%	1432	97.6%	13494	93.9%	952	98.4%
Cybec Vet AntiVirus	87	98.9%	665	100.0%	99.6%	1433	96.8%	13000	91.3%	944	97.6%
Data Fellows FSAV	88	100.0%	665	100.0%	100.0%	1497	99.2%	14244	100.0%	1006	99.7%
Dr Solomon's AVTK	87	98.9%	665	100.0%	99.6%	1465	98.9%	13500	94.8%	961	98.7%
EliaShim ViruSafe	n/a	n/a	659	99.6%	n/a	1362	93.1%	13243	91.7%	946	97.9%
ESET NOD32	88	100.0%	665	100.0%	100.0%	1461	98.5%	13813	96.4%	970	98.8%
Kaspersky Lab AVP	88	100.0%	665	100.0%	100.0%	1501	99.5%	14244	100.0%	1015	100.0%
NAI NetShield NT	88	100.0%	656	99.4%	99.6%	1449	97.9%	13275	88.3%	970	98.5%
Norman Virus Control	n/a	n/a	665	100.0%	n/a	1435	96.8%	13498	93.9%	973	97.1%
Sophos SWEEP	88	100.0%	665	100.0%	100.0%	1454	98.2%	13748	96.1%	959	98.3%
Symantec Norton AntiVirus	75	85.2%	665	100.0%	94.9%	1421	96.0%	13500	94.8%	948	98.1%

Command AntiVirus v4.51

ItW Overall	100.0%	Macro	99.2%
ItW Overall (o/a)	94.9%	Polymorphic	93.9%
ItW Boot	100.0%	Standard	98.4%

The third VB 100% award in a row – what is the world coming to? Proof that improvement is possible comes in the all-new incarnation of *F-PROT*. Although a new version of the product, there were no stability problems to be seen with *Command's* packaging of the *F-PROT* engine. Somewhat surprisingly, given *F-PROT's* reputation, macro detection was not 100%. This was partly due to the A97M/AccessiV variants, though to be fair it does not claim to detect these. More surprisingly, it missed the macro portion of Navrhar. The latter is possibly classifiable as a dropper, yet still falls well within the 'should find' category.

A new addition to *Command AntiVirus* (*CSAV*) is an on-access scan for boot sectors, but as yet, strange boot configurations are enough to confound detection and the detection of disk changes is also less than admirable. The on-demand scanning of diskettes is a joy, with the exception of those selfsame strange file systems adding options to the process, which might be considered confusing.

Since its last outing on this platform *CSAV's* polymorphic detection has almost doubled in percentage terms, from 47.6% to 93.9%, and is now back in the realms of the respectable. Some improvement could perhaps be made to the speed, and the on-access overhead is certainly over the desired value. That said, there has been considerable positive feedback on *CSAV's* development since this version was first released. The future may well be promising

Cybec Vet AntiVirus v9.80

ItW Overall	100.0%	Macro	97.4%
ItW Overall (o/a)	99.6%	Polymorphic	94.8%
ItW Boot	100.0%	Standard	97.9%

The rash of perfect on-demand detection against the In the Wild test-sets continues apace with *Vet*. Notorious for its speed, this antipodean offering did not fail to impress on this front. It was third against the Clean test-set, as well as being ahead of average in diskette scanning and least burdensome in the overhead category.

In fact, the top two performers in the overhead category produced one of the more impressive results in this review, in that rather than slowing down XCOPY, the on-access scanners caused the process to become faster. The developers of both these products attribute this unlikely result to their decision to implement on-access scanning as a file-system filter rather than as a service.

Vet performed a little oddly – on a par with *CSAV* in this respect – in that, on-access, it detected all the samples in the Standard test-set, despite failing to do so on-demand. This strangeness was heightened by the reverse being true in some other test-sets and equality prevailing in others.

As far as boot viruses were concerned, inconsistency was noted again, in the missing of ABCD on-access. On-demand, affairs were much happier than in the last test for *Vet*. On that occasion, all non-standard boot sectors were undetected, but this time they were discovered with no problems at all.

Data Fellows F-Secure Anti-Virus v4.01aβ

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	99.7%

A chimeric breed of *AVP* and *F-PROT*, the *Data Fellows* product has proven unpredictable and bothersome in *Windows 95* reviews, and this trend seems likely to continue. The interbreeding of the two products has certainly given rise to a perceptive beast, though slightly less so than *Kaspersky Lab's* offering, and not without its concomitant problems. As a relatively new product, however, teething problems are to be expected.

Two engines obviously add to the burden imposed upon operations. With on-access scanning enabled, copy operations took four times longer, while other scanning operations were also slow. More disturbing was the logging of infections, which produced double reports for some infected objects, one report for others, and in some uninfected objects resulted in an error message when *AVP* attempted to scan after *F-PROT*.

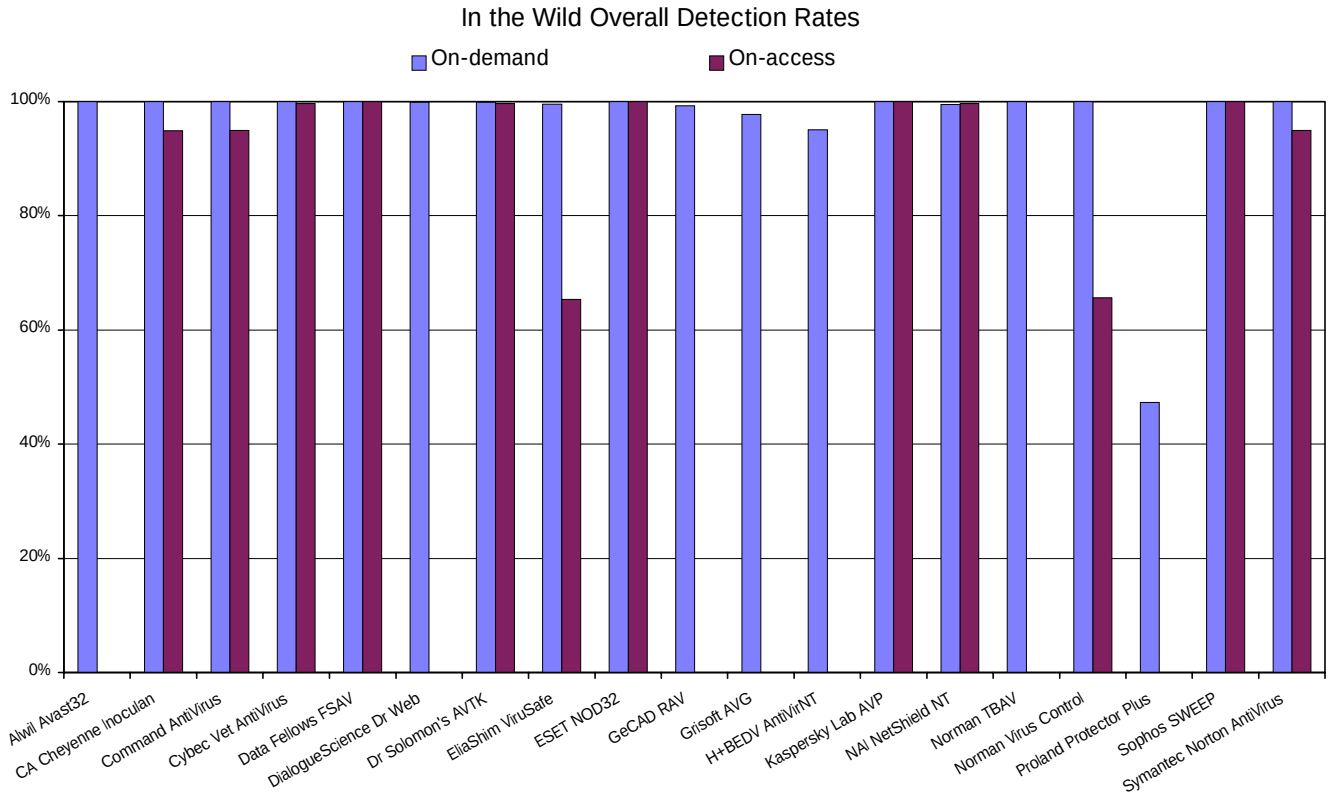
Perhaps due to the Medusa-like ugliness of these reports, *Data Fellows* seems most unwilling to allow log files to be produced, and the tester's tender sensibilities were further shielded by *F-Secure's* (*FSAV*) ability to crash when logs were redirected to a file masquerading as a printer.

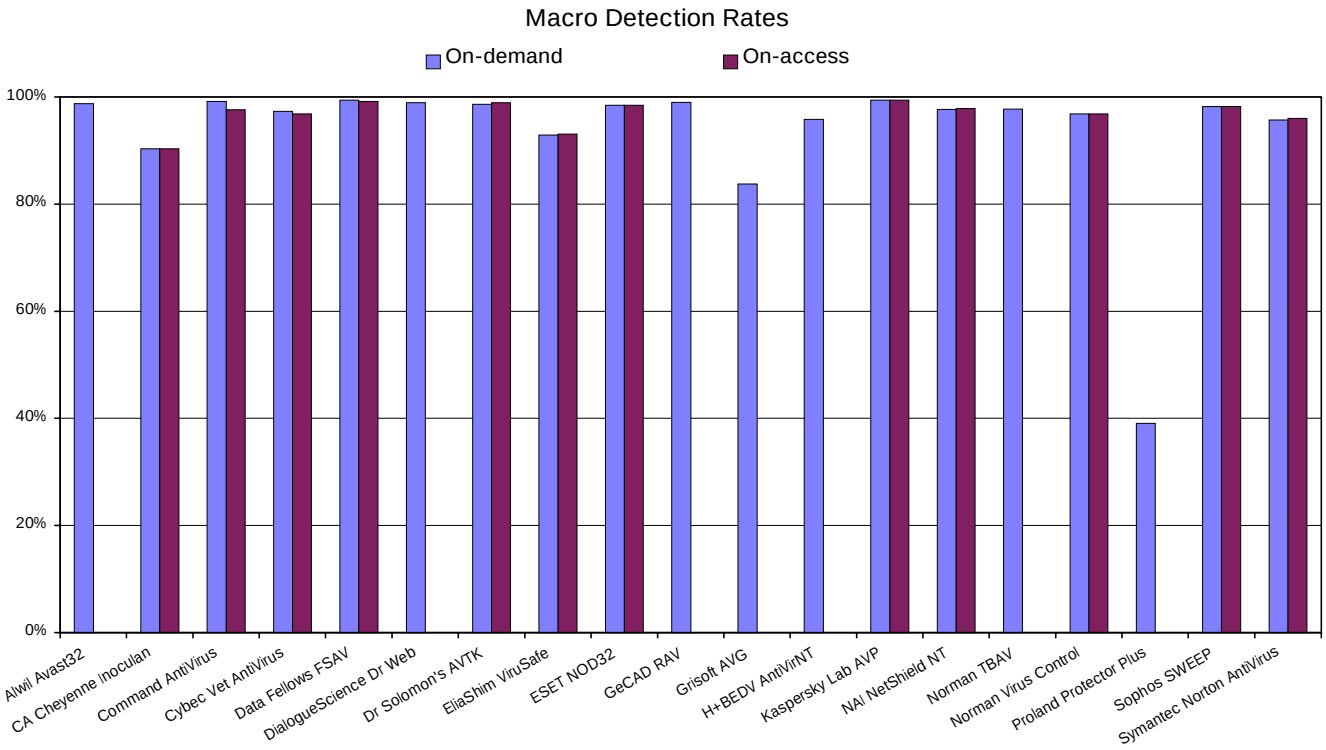
This activity required testing of the maim and kill variety, the program being set up to delete any viral files found, with those remaining taken to be missed samples. Unfortunately, the two 'heads' of the program are often at odds as to whether a sample is viral. The result was a file not deleted but renamed – the first letter of the extension being replaced with V. Not entirely unreasonable it might be thought, until it is realized that Navrhar infects VxDs, files with an extension which tells *FSAV* the file has already been scanned! Thus, although *AVP* can detect the viral VxD, it passes as undetected by the *Data Fellows* product.

Boot sector testing was not exactly a pleasure to see, with the on-access component reducing *NT* to a blue screen on occasion. Problems were also encountered with multiple messages and changeover detection. With a beta version being tested, it is to be hoped that many of these problems have been addressed in the full release. *FSAV* still received a VB100% award despite all these woes.

DialogueScience Dr Web v4.01β

ItW Overall	99.9%	Macro	98.9%
ItW Overall (o/a)	n/a	Polymorphic	100.0%
ItW Boot	98.9%	Standard	99.7%





Dr Web has all the attributes of a mighty club – somewhat slow, a little old-fashioned looking but very effective none-the-less. Heuristics are the order of the day at *Dialogue-Science*, and effective they are indeed. Misses were due mostly to unscanned extensions, though the two W97M/Class variants escaped. The downside of this reliance on heuristics is the announcement of 14 false positives against the Clean test-set, together with the slowest performance in that test – over thirty times longer to perform the scan than the fastest credible scanner.

A VB 100% award eluded *Dr Web* by one missed boot sector virus, Lilith, a non-detection which should be easily rectified. On-demand diskette scanning also proved a little burdensome in that the scan target was reset after each scan had been performed, necessitating individual selection for the 88 disks. A great plus point, from a reviewer and user point of view, was that despite being declared a beta, *Dr Web* showed no signs of instability whatsoever.

A disappointing omission, although admittedly requiring a great deal of programming to remedy, was the lack of an on-access component in this new version.

Dr Solomon's AVTK v7.85

ItW Overall	99.9%	Macro	98.7%
ItW Overall (o/a)	99.6%	Polymorphic	94.8%
ItW Boot	98.9%	Standard	98.7%

The last of a dying breed, the mighty figure that once was *Dr Solomon's* is currently being fitted to *NAI's* Procrustean empire. As *AVTK 8* will never see the light of day, this possibly marks the final outing for the *NT ToolKit* as a fully supported product. As it was, the end came not with a bang but with a whimper, as the missing of Ornate – a virus it has detected in several previous tests – in the boot sector tests denied the product a VB 100% award.

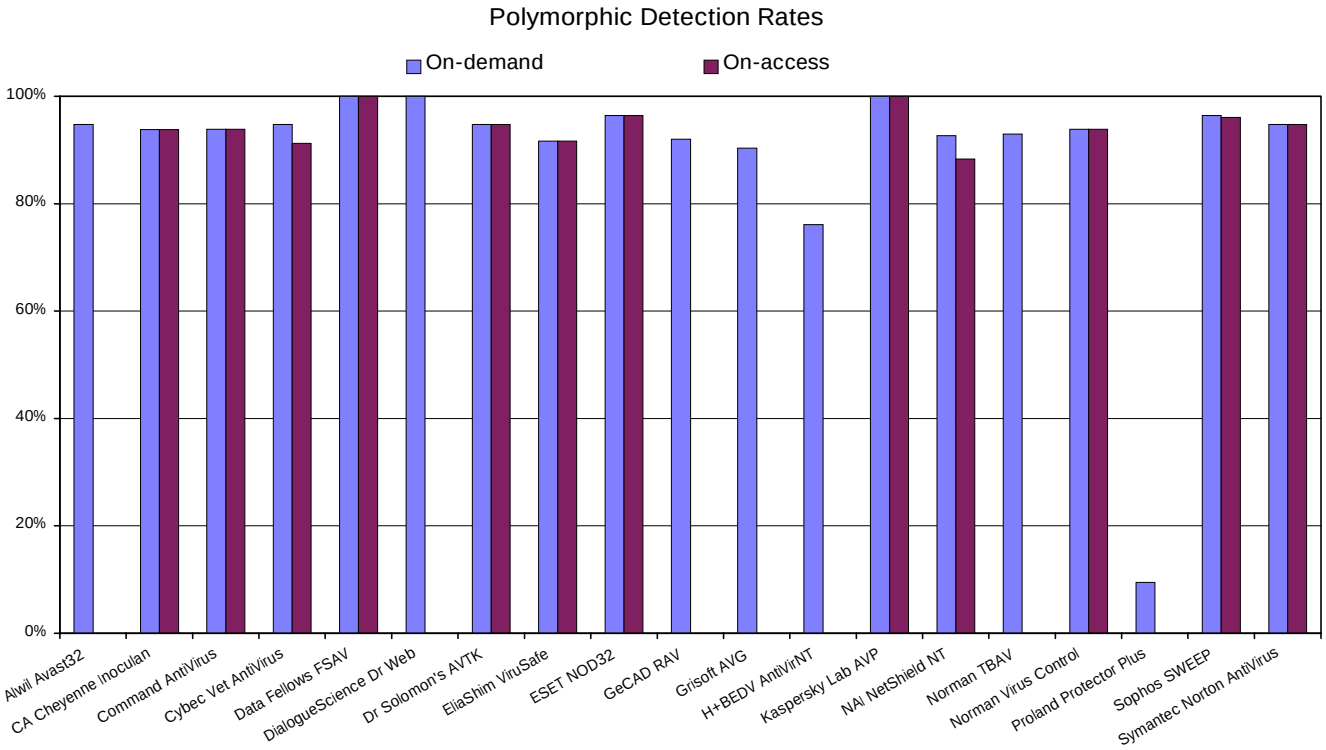
A succession of misses in other areas did more than this, pushing the results well into the mid-range of the detection league. On-access overhead was an area where *AVTK* still remains impressive, not quite up with the best, but only 20% up on times with this component unloaded.

The areas *NAI* hopes to improve on were also behaving at their worst. The selection of subdirectories for scanning proved a Gordian knot in its complexity – *AVTK* twice admitted defeat, with error messages composed entirely of ASCII graphical characters when scans were being prepared. Boot sector scanning was a much more pleasant affair, but the real interest now lies in the alchemical marriage of *Dr Solomon's* and *NAI*.

EliaShim ViruSafe v2.7

ItW Overall	99.5%	Macro	92.9%
ItW Overall (o/a)	n/a	Polymorphic	91.7%
ItW Boot	98.9%	Standard	97.9%

ViruSafe is soon to be enhanced, providing a more complete *NT* product, although the current offering displays no major flaws. Detection was not stunning in any category, though not appalling either – the exception being on-access boot sector scanning which is not supported in any way, shape or form. On-demand detection rates have improved over previous tests, but the perennial favourite Hare.7610 still evades *ViruSafe's* detection routines.



Speed-wise, the hard disk rate continues to be at the very respectable end of the field and now with a much reduced false positive rate, evidence of the continuing development effort. An application which escapes great discussion by doing what it sets out to do and exhibiting no bizarre traits.

ESET NOD32 v1.06

ItW Overall	100.0%	Macro	98.5%
ItW Overall (o/a)	100.0%	Polymorphic	96.4%
ItW Boot	100.0%	Standard	98.8%

ESET has not featured in an *NT* comparative with this dedicated 32-bit product – a situation which often causes trepidation in the reviewer's psyche. The overall, dark cyber-creature theme of the artwork is muted here, but cosmetics are not the prime concern of this review.

The review process was, despite unfamiliarity with the product, a pleasant one overall; the interface being simple to control and effective. On-demand diskette scanning was particularly well-implemented, and with both varieties of boot check there were no problems with either odd boot sectors or disk change detection. Speed was at the better end of the range but on-access overhead was rather high.

Detection, too, was definitely more respectable than many new implementations have managed, earning *NOD32* a VB 100% award on its first appearance on this platform. Results were especially impressive on-access, only lagging slightly behind the *AVP*-powered leaders. *ESET* reports that it is currently busy with translation of its manuals and documentation, and a *VB* standalone review is forthcoming.

GeCAD RAV v6.01

ItW Overall	99.3%	Macro	99.0%
ItW Overall (o/a)	n/a	Polymorphic	92.1%
ItW Boot	100.0%	Standard	93.7%

This version of *RAV* submitted for testing had several notable differences from those seen previously. The addition of some violent colour schemes was quite eye-catching, and the claim to support thirty-four languages marginally more remarkable.

In a more relevant vein, there were also improvements apparent in the internal workings of the program and its detection capabilities. Three incompletely detected viruses against the In the Wild test-set came between it and a VB 100% award. 99.3% overall ItW detection rate is a large and desirable improvement compared to 82.8% in March. Macro detection was second only to *FSAV* for the most improvement, up from 64.3% to 99.3%, and the overall improvements hoist *RAV* firmly toward the top-end of detection performance.

Improvements are still to be had, on the other hand, with nine false positives still raising their heads against the Clean test-set. Lack of an on-access component was none too favourable either, and despite the full detection of boot viruses on-demand, the interface was tortuous at best. Repeated scans required clicking through the selection of a scan, the ignoring of a 'there is something missing' error message, and the choice of various different buttons from a large selection.

Scan speeds are a little sluggish, yet with the current rate of improvement *RAV* is certainly a product to watch.

	Scanning Speed						On-access Overhead (default configuration)	False Positives
	Diskette - Clean		Diskette - Infected		Hard Drive - Clean			
	Time (seconds)	Throughput (KB/s)	Time (seconds)	Throughput (KB/s)	Time (min:sec)	Throughput (KB/s)		
Alwil Avast32	65	15.0	100	11.8	29:16	304.2	n/a	1
CA Cheyenne Inoculan	159	6.1	184	6.4	5:44	1552.7	92.9%	1
Command AntiVirus	124	7.9	133	8.9	3:50	2322.2	123.1%	1
Cybec Vet AntiVirus	61	16.0	66	17.9	1:35	5622.2	-23.9%	1
Data Fellows FSAV	162	6.0	300	3.9	7:53	1129.2	304.1%	0
DialogueScience Dr Web	106	9.2	105	11.3	40:55	217.6	n/a	14
Dr Solomon's AVTK	64	15.2	78	15.2	3:26	2592.8	19.7%	0
EliaShim ViruSafe	59	16.5	65	18.2	2:04	4307.4	93.1%	4
ESET NOD32	57	17.1	65	18.2	2:21	3788.0	154.7%	0
GeCAD RAV	64	15.2	94	12.6	9:43	916.1	n/a	7
Grisoft AVG	63	15.5	71	16.6	2:21	3788.0	n/a	51
H+BEDV AntiVirNT	62	15.7	89	13.3	2:42	3297.0	n/a	4
Kaspersky Lab AVP	61	16.0	67	17.6	5:17	1684.9	172.5%	3
NAI NetShield NT	58	16.8	45	26.3	15:55	559.3	141.8%	0
Norman TBAV	50	19.5	43	27.5	1:12	7418.2	n/a	0
Norman Virus Control	63	15.5	66	17.9	4:26	2007.9	171.6%	0
Proland Protector Plus	62	15.7	85	13.9	1:07	7971.8	n/a	1
Sophos SWEEP	54	18.0	65	18.2	2:25	3683.5	-18.9%	0
Symantec Norton AntiVirus	119	8.2	134	8.8	3:24	2618.2	49.3%	0

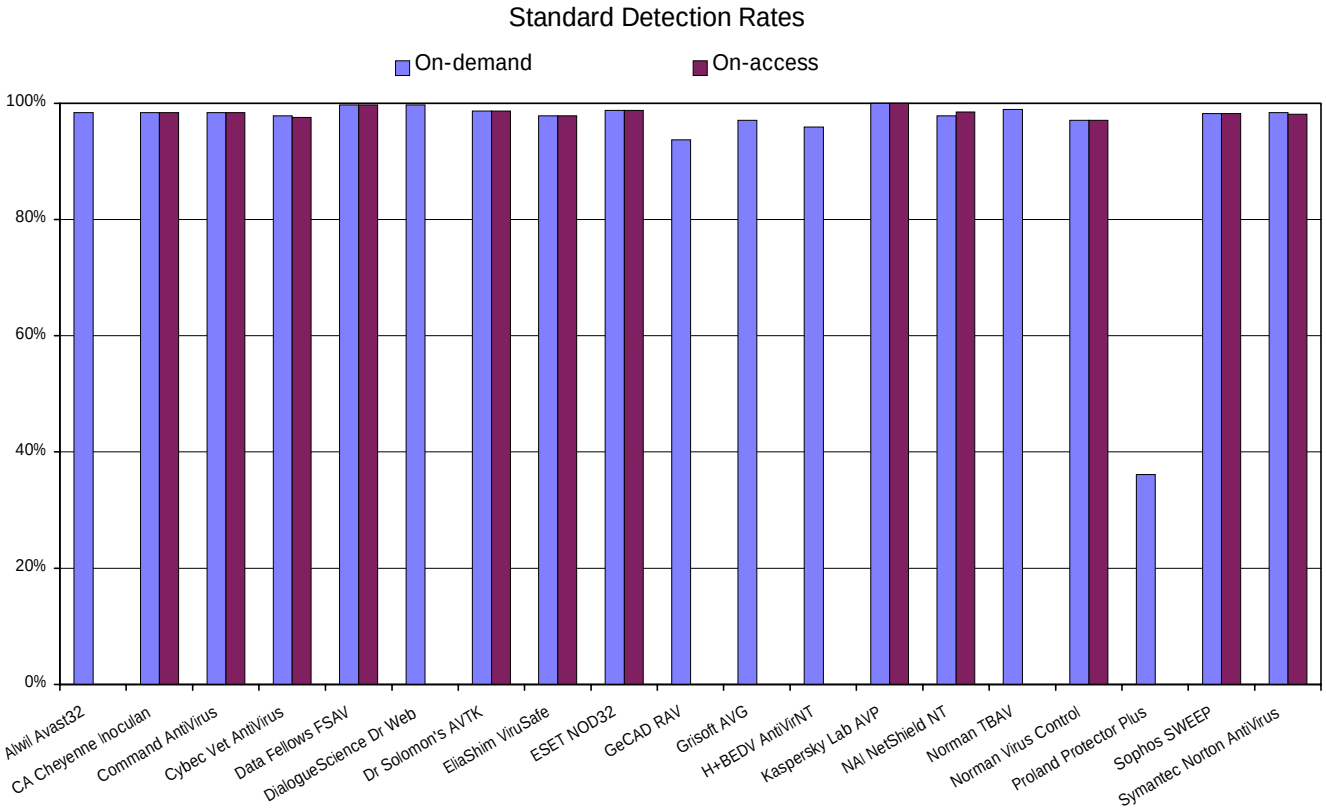
Grisoft AVG v5.0v16

ItW Overall	97.7%	Macro	83.8%
ItW Overall (o/a)	n/a	Polymorphic	90.4%
ItW Boot	83.0%	Standard	97.1%

Shipping as a general-purpose Win32 product, its VxD on-access scanner means *AVG* provides no on-access protection under *NT*. Topping the false positive count with 51 in total – all attributed to the Tentacle virus – *AVG* missed only two samples in the ItW File test. Ironically, these were both samples of Tentacle.10634! This might well be a simple problem with the Tentacle detection string. More problems were apparent in the boot sector tests.

AVG was unable to deal with strange boot sectors in its on-demand tests. It was also unable to detect Hare.7786 and Hare.7610 – both of which have caused problems for many in the past – and that Methuselah of viruses, Natas.4744. In addition to these technical problems, scanning more than one diskette was roundabout and surely off-putting to anyone other than an ardent reviewer.

Grisoft has included some extras not found elsewhere, including a single stepping version of their emulator, and the presentation standards overall are high. Since its first appearance, detection rates have increased but not as remarkably as those of *RAV*. However, *AVG* had the worst boot sector virus detection of the real scanners tested this



issue, finding only 83% of In the Wild Boot viruses. Detection results are less than acceptable in general and it is to be hoped that further redirection of effort towards the internals of the product will reap greater improvements.

H+BEDV AntiVirNT v1.07

ItW Overall	95.0%	Macro	95.9%
ItW Overall (o/a)	n/a	Polymorphic	76.1%
ItW Boot	97.7%	Standard	95.9%

H+BEDV's product provided installation problems, proving to be more paranoid than was healthy for its own good. The first version tested was in English but, upon activation, it failed its integrity check, proclaiming that it was infected and terminating. A newer, post deadline, version was tested and therefore it must be noted that *AntiVir's* results are not directly comparable with other products, reflecting signatures from 30 July.

That said, detection rates were (while not particularly bad in general) certainly under par when it came to the Polymorphic test-set, with a mere 76.1% detection rate. Three of *AntiVir's* four false positives were suspected 'virgen' productions, and correction of this might prove to be a simple tweak. On-demand detection of boot viruses, too, could benefit from some attention, partially due to the product missing samples of Moloch and Lilith and also due to the four keystrokes required for each scan of an infected object. Another offering lacking an on-access scanner, *AntiVir* is looking overdue for a revamp.

Kaspersky Lab AVP v3.0

ItW Overall	100.0%	Macro	99.5%
ItW Overall (o/a)	100.0%	Polymorphic	100.0%
ItW Boot	100.0%	Standard	100.0%

With a very good recent history, it was no great shock when *AVP* qualified for another VB 100% award. However, it was surprising that it missed WM/Mortal.A, but less so that the other missed virus was W97M/Kitty.B – a recent addition to the test-set.

Despite these detection rates, *AVP* was not without some problems. Three false positives and large on-access overheads were not unexpected with the intensive scanning to which *AVP* subjects files. While boot sector scanning was exemplary on-demand, matters were different on-access, the traditional *NT* sticking point. Alerts and change detection were at their seemingly most random, and at one point, perhaps driven to paranoia by detection of too many viruses, *AVP* denied access to the A: drive permanently. This required a reboot to restore things to normality.

Network Associates NetShield NT v3.14a

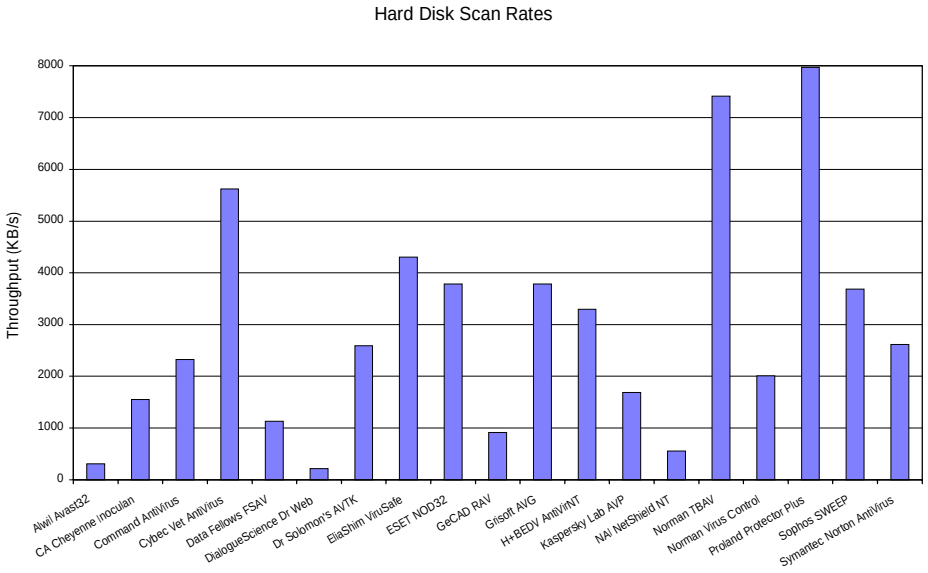
ItW Overall	99.5%	Macro	97.7%
ItW Overall (o/a)	99.6%	Polymorphic	92.7%
ItW Boot	100.0%	Standard	97.9%

Having spent the riches of Croesus on the *Dr Solomon's* engine, this must be the first occasion when *NAI* is hoping to detect fewer viruses than its erstwhile nemesis. These

results do not disappoint on that front. *VirusScan's* next appearance in a *Virus Bulletin* comparative review might well incorporate the *Dr Solomon's* engine, and is an interesting arrival to anticipate.

VirusScan is certainly not as fast as *AVTK*, nor indeed most of the tested products, yet it still managed to produce a seemingly miscounted number of files against the Clean test-set. Overheads were somewhat above average, though floppy disk scan rates were among the best.

An area where *NAI* can claim victory is the boot sector, where detection rates were 100%, something of an improvement upon a notable, if untypical, past performance. The results were good but the interface in the on-demand and on-access versions was still less than perfect. On-demand scanning stopped with the scan start button still depressed, requiring a pause action to allow a new scan even when scanning was clearly complete, while on-access disk change detection and messaging were erratic.



Norman ThunderByte AntiVirus v8.07

ItW Overall	100.0%	Macro	97.7%
ItW Overall (o/a)	n/a	Polymorphic	93.0%
ItW Boot	100.0%	Standard	98.9%

Norman ThunderByte (*NTBAV*) is, as always, vying with *Vet* for the fastest 'real' scanner and on this occasion comes out in front. Speeds on hard disk scanning were more incredible than respectable, more so because it was clear that *NTBAV* was performing a great deal of heuristic analysis. This was visible if the more detailed log file options were selected, when, typically, a half dozen lines of analysis for each virus were produced for the report file.

Floppy disk scanning was in the same speedy league, yet the quickness can only be appreciated if sacrifices are not made. With no false positives, complaints cannot be made on this front, though the lack of an on-access scanner is certainly an oversight. In the grand scheme however, detection rates are the key.

Here again there can be few complaints, since *Norman ThunderByte* is a happy recipient of a VB 100% award. On the negative side, polymorphic detection is worrying at 93% – an area where perhaps speed is causing detection to be cut a little. All in all, *NTBAV* is a virus detector which, unlike many, could afford to become a little more tardy if detection were to increase, and yet again is in need of an on-access component.

Norman Virus Control v4.53

ItW Overall	100.0%	Macro	96.8%
ItW Overall (o/a)	n/a	Polymorphic	93.9%
ItW Boot	100.0%	Standard	97.1%

With much talk of the need for on-access components comes *Norman Virus Control* (*NVC*), which has recently revamped its on-access process. In the past, only macros were protected by the CatsClaw utility but the new version replaces this with a service which scans all file operations but not yet boot sectors. This is only mentioned in passing in the help files for the on-demand scanner, and is otherwise hidden away on the service manager console.

New additions to a product are often prone to hiccups but, thankfully, *NVC* retains its reputation for complete stability. Detection rates were sufficient to gain a VB 100% award, with its main weakness against the Polymorphic test-set. Unusual in this review, results were identical on-access and on-demand, a feature which is linked with the unified service-oriented nature of the *NVC* scanner.

Slight niggles did occur – the on-demand scanning interface is slightly complicated by its need for several clicks, and the overhead for the on-access scanner is rather high.

Proland Protector Plus v6.5

ItW Overall	47.3%	Macro	39.1%
ItW Overall (o/a)	n/a	Polymorphic	9.5%
ItW Boot	28.4%	Standard	36.1%

This is the first appearance of *Proland Software's* product in a Virus Bulletin review. Completely unheard of prior to receipt, it turned out to be very disappointing. References to real scanners earlier in the review may have confused some readers, but it seemed unfair to compare the products discussed to the Augean stable proffered by *Proland*.

Speedy it may be, but the cynical will immediately suggest that the program is doing so little work that anything other than speed would be a miracle.

The virus identities used here seem to have stabilized some two years or so ago – with such wonders of the ancient world as Empire.Monkey.B being too tricky for detection. The figures speak for themselves.

Sophos SWEEP v3.11

ItW Overall	100.0%	Macro	98.2%
ItW Overall (o/a)	100.0%	Polymorphic	96.4%
ItW Boot	100.0%	Standard	98.3%

Alphabetically, *SWEEP* has the dubious honour of following *Protector Plus*, and returns us to the levels of detection expected of a late-nineties anti-virus product. The second of the products to speed up file transfer when used on-access, by some 20%, *SWEEP* is among the faster of the hard and floppy drive scanners too.

The usual worries concerning speed seem to be without foundation in *SWEEP's* case, with a VB 100% award and good detection, though, as with so many of the products this month, polymorphic detection is lower than in the past. Mid infectors continue to make up a good portion of the missed samples in the Standard test-set, though a new version of *SWEEP* in the pipeline offers the possibility that these might in future be detected in a standard scan.

Floppy disk scanning was the fly in the ointment for *SWEEP*, though not for the usual reasons. Interface problems were the key, with the lack of a 'hot' scan-start button and the remarkably small size of the results window being areas where interface design could be improved.

Symantec Norton AntiVirus v4.08

ItW Overall	100.0%	Macro	95.8%
ItW Overall (o/a)	94.9%	Polymorphic	94.8%
ItW Boot	100.0%	Standard	98.4%

Being the last in the line up is an unenviable position for *Symantec's* product, attention compounded by the recent standalone review (see *VB*, August 1998, p 21). Tests against the Clean test-set demonstrated no false positives in an unobtrusively average time, though floppy disk scanning was not as fast as might be hoped. Overheads, on the other hand, were not huge, a matter of great importance to users.

NAV was the final recipient of a VB 100% award, meaning that eleven out of nineteen products qualified for one in this review. Out of the wild and on-access *NAV* looked slightly less convincing than many of the other products, with detection of less than 95% in both the Polymorphic test-set and overall In the Wild on-access.

Conclusion

In summing up, the trend is one of continued good detection against the ItW test-set, with some already noted exceptions. Stability does appear to be a problem with some products, and in the case of *Inoculan* at least, cannot be ascribed to the introduction of new code. In other categories, detection rates are down on past outings, especially in the Polymorphic test-set. The inclusion of new samples – several of them with extensions of SCR, MDB or VXD which are not commonly listed as default file types to scan – contributed here.

The submission date for this review passed shortly before the CIH and Marburg scares were rife, but after the two viruses were known to exist in the field. In light of the subsequent festival of updates and press releases it is interesting to note which products detected these viruses in their submitted versions, if only to mention some of the pitfalls involved with them.

Of the tested software only *DrWeb*, *AVP* and *FSAV* detected all samples of CIH and Marburg which were supplied to them on-demand. The *AVP* engine was aware of the signature patterns involved and acted on them, while *DrWeb* used its heuristic prowess to good effect. *FSAV* includes the *AVP* engine, thus benefitting from *Kaspersky Lab's* speedy inclusion of the virus in its detection library.

Of the more partial detections, *NVC* detected all samples of CIH, whilst *NTBAV* and *NAI's NetShield* detected the majority – missing samples which, although common *Microsoft*-produced files were used as a host, do not strictly follow PE header guidelines. These products are clearly sticklers for the *Microsoft* way to a greater extent than *Microsoft* itself. As for Marburg, both *NOD32* and *SWEEP* were aware of the virus, but neither was able to detect all the samples. Marburg performs several different entry-point modifications depending upon the host file, and neither product seemed to take full account of this.

So, with an extra two months of planning in hand, the next comparative review should, we hope, see most of these problems resolved. On the other hand, that will be the first *Windows 98* comparative, and might include samples of the first Java virus in the test-set – opening a whole new Pandora's box of possible woes.

Technical Details

Test Environment: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, running *Windows NT v4.0 (SP3)*. The workstations could be rebuilt from disk images and the master copy of the test-set was held on a CD-ROM. All timed tests were run on one workstation.

Speed and Overhead Test-sets: Clean Hard Disk: 5500 COM and EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk.

Virus Test-set: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/199809/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.