COMPARATIVE REVIEW

Scanning on NT

The last time we ran an *NT* comparative review was in September 1997, where we predicted the wider deployment of *NT* as a desktop operating system, rather than as a server platform (see *VB*, September 1997, p.10). It appears we were right, and this current comparative concentrates again on *NT* workstation. Nineteen products were submitted for review, and, as expected, an on-access scanning option is fast becoming standard. Several companies which had not included an on-access scanner with the product submitted for this test claim that the option is scheduled for addition in the next release.

Testing, testing

All tests were run from the Administrator usercode on a standalone *Windows NT 4.0* workstation with Service Pack 3 installed. Boot sector detection tests were run simultaneously with the file-scanning tests, but on another machine, to save time. Sector-level image backups were used to restore the workstation between tests.

The usual *Virus Bulletin* test-sets – In the Wild File and Boot, Macro, Polymorphic and Standard – were used in this review. The ItW sets were updated to the December 1997 WildList, which was the current listing at product submission date (5 January). The standard Clean test-set was used for on-access overhead and on-demand scanning time tests. Generally, default settings were used throughout with the exception that on-access components, where available, were disabled during all on-demand tests. In most cases log files were checked in order to collate detection results. With some scanners it was necessary to use the 'delete infected files' option or to 'quarantine' files.

As in most real-world operation, the scanners faced a large number of uninfected programs in the main speed tests. Here the scanner in question is the foreground application, with *NT's* scheduling set to 'Maximum boost for the foreground application', and no other programs running. This procedure also acts as the false positive test, in which no viruses should be reported.

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

Alwil AVAST32 v7.70.12 5 Jan 1998

ItW Overall	99.2%	Macro	100.0%
ItW Overall (o/a)	n/a	Polymorphic	95.4%
ItW Boot	100.0%	Standard	100.0%

AVAST32 started out with perfect detection of the ItW Boot set on-demand. The Standard and Macro sets were also perfectly detected, a slight improvement in the macros over the last *NT* comparative. This places *Alwil* with only four other products which scored over 99% In the Wild Overall in this comparative. A good improvement was seen against the Polymorphic test-set.

Although *Alwil* provides an on-access scanner, we could not test its detection rate. This is because, apart from its boot virus detection, it only intercepts attempts to execute potentially infected objects and our testing facility is set up to run tests where the whole system needs rebuilding between each sample to ensure an accurate test.

This was by far the slowest of the scanners tested, six times slower than its nearest competitor, and fifty times more sedentary than its speediest competitor. *Alwil* has opted to give *AVAST32* a very low thread priority, to the extent that a full scan should be almost invisible in terms of overhead on other applications. The clean scan did show up a pair of false positives however, so perhaps this area will be the next to see some very fine tuning.

Cheyenne Inoculan v4.04 15 Jan 1998

ItW Overall	98.8%	Macro	93.1%
ItW Overall (o/a)	93.8%	Polymorphic	90.9%
ItW Boot	98.9%	Standard	99.6%

The on-demand boot test slipped up on the Hare.7610 sample, and caused non-fatal errors on the thirteen samples with less than standard disk formats caused by the virus' meddlings. This slight deviation from perfection was a common thread running through *Inoculan*, and there is a tiny slip from the In the Wild scores of the last outing.

There were improvements – healthy against the Polymorphic test-set and slight in the other on-demand tests. Presentation is of course a strong point, and it must be admitted that there were many features in the package which a workstation-only review cannot address. The missing of small numbers of samples across the board points to a weakness in identities rather than overall mechanics, which is all the more perplexing since this was the most recently built product of all those tested.

Despite a slight difficulty in logging it, on-access scanning was fully supported, and produced similar results to those of the on-demand option. One remarkable feature is that the Polymorphic set was slightly better detected on-access than on-demand. File, Macro and Standard tests dropped two samples fewer than their on-demand counterparts, a creditable result indeed. Scanning speed was at the slower end of the pack, and a brace of false alarms were reported.

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	89	100.0%	629	98.8%	99.2%	744	100.0%	12998	95.4%	887	100.0%
Cheyenne Inoculan	88	98.9%	643	98.8%	98.8%	691	93.1%	12699	90.9%	883	99.6%
Command F-PROT Pro	89	100.0%	621	98.2%	98.8%	744	100.0%	7066	47.6%	887	100.0%
Cybec VET	76	85.4%	651	100.0%	94.9%	744	100.0%	13500	100.0%	887	100.0%
Dr Solomon's AVTK	89	100.0%	651	100.0%	100.0%	744.00	100.0%	13500	100.0%	887	100.0%
EliaShim ViruSafe	86	96.6%	649	99.9%	98.7%	733	98.5%	12823	93.5%	878	99.4%
GeCAD RAV	77	86.5%	507	80.9%	82.8%	485	64.3%	13494	98.1%	821	92.6%
Grisoft AVG	68	76.4%	514	81.9%	80.0%	663	88.3%	11026	81.6%	629	78.6%
H+BEDV AntiVir/NT	87	97.8%	586	92.3%	94.2%	723	96.4%	11455	83.1%	849	96.5%
IBM AntiVirus	87	97.8%	647	99.4%	98.8%	744	100.0%	13000	96.3%	887	100.0%
Intel LANDesk Virus Protect	79	88.8%	623	97.9%	94.7%	744	100.0%	12825	92.5%	861	97.8%
iRiS AntiVirus	88	98.9%	643	98.8%	98.8%	690	93.0%	12699	90.9%	883	99.6%
KAMI AVP	76	85.4%	651	100.0%	94.9%	744	100.0%	13499	99.1%	887	100.0%
McAfee VirusScan	1	1.1%	651	100.0%	65.8%	744	100.0%	13441	98.7%	870	98.9%
Norman ThunderByte	89	100.0%	644	99.8%	99.8%	741	99.6%	13496	98.1%	878	99.2%
Norman Virus Control	89	100.0%	633	99.4%	99.6%	740	99.5%	1296	94.2%	881	99.7%
Sophos SWEEP	89	100.0%	647	99.4%	99.6%	744	100.0%	13495	99.0%	885	99.7%
Symantec Norton AntiVirus	89	100.0%	611	97.0%	98.1%	735	98.5%	11501	84.3%	872	99.1%
Trend Micro PC-cillin NT	84	94.4%	625	98.1%	96.8%	744	100.0%	12883	93.8%	861	97.8%

This leaves the boots, where *Cheyenne's* product was confused by uncommon disk formats, but managed to produce an error for both format and virus, which is to its credit. Consistency between on-demand and on-access detection was maintained since other than these only Hare.7610 was missed. *Inoculan* falls in that middle ground where improvements and declines are as noticeable as they are important.

Command F-PROT Professional v3.01/2.27a

ItW Overall	98.8%	Macro	100.0%
ItW Overall (o/a)	64.2%	Polymorphic	47.6%
ItW Boot	100.0%	Standard	100.0%

F-PROT's speed is among that of the top few and it makes no spurious detections; hardly conversation pieces. Close to the coveted perfect ItW Overall score, missing a handful of file viruses knocked *F-PROT* back to mid-field. The great bane of its detection prowess is, however, the polymorphics. This situation is getting worse monthly, moreover, and the suspicion must be that the imminent v3.0 engine is being developed at the expense of maintaining the older of the species. Standard, Macro and Boot samples, all perfectly detected, back up this theory, requiring not so much an advanced emulator as good scan strings usable by the older *F-PROT*. The odd formats caused no problems in the boot virus tests, though Paula_Boot did throw up an 'unable to read' error on top of a virus alert.

Affairs are not so promising on-access, where boot sector scanning was ignored completely. Polymorphic detection is again a trifle over the on-demand rate with similar comments applying as were warranted by *Inoculan*. Other detection rates dropped due to the need for speed rather than massive detection efficiency. A product which shows its age, and will hopefully have a worthy successor.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	80	89.9%	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Cheyenne Inoculan	75	84.3%	643	98.8%	93.8%	690	93.0%	12750	91.2%	883	99.6%
Command F-PROT Pro	0	0.0%	621	98.2%	64.2%	733	98.5%	7082	47.7%	798	92.6%
Cybec VET	79	88.8%	622	98.4%	95.1%	744	100.0%	12998	95.4%	867	97.9%
Dr Solomon's AVTK	89	100.0%	651	100.0%	100.0%	744	100.0%	13500	100.0%	887	100.0%
EliaShim ViruSafe	0	0.0%	649	99.9%	65.3%	731	98.2%	13163	95.4%	878	99.4%
IBM AntiVirus	87	97.8%	647	99.4%	98.8%	744	100.0%	13000	96.3%	887	100.0%
Intel LANDesk Virus Protect	69	77.5%	623	97.9%	90.9%	744	100.0%	12824	92.5%	861	97.8%
McAfee VirusScan	88	98.9%	530	82.9%	88.4%	688	91.7%	6385	44.7%	767	88.6%
Norman Virus Control	n/a	n/a	424	67.6%	n/a	717	96.6%	7997	44.4%	632	69.1%
Sophos SWEEP	89	100.0%	647	99.4%	99.6%	744	100.0%	13495	99.0%	885	99.7%
Symantec Norton AntiVirus	70	78.7%	611	97.0%	90.7%	743	99.5%	11499	84.3%	841	97.2%
Trend Micro PC-cillin NT	n/a	n/a	625	98.1%	n/a	744	100.0%	12883	93.8%	861	97.8%

Cybec VET v9.61

ItW Overall	94.9%	Macro	100.0%
ItW Overall (o/a)	95.1%	Polymorphic	100.0%
ItW Boot	85.4%	Standard	100.0%

The product for the people to whom velocity is almost everything, *VET* churned through the 500 MB of the Clean test-set in a mere 102 seconds, yet still showed an impressive on-demand detection rate. The detections against the In the Wild File, Standard, Polymorphic and Macro test-sets all gained the much sought-after full marks, so far so good.

Those who crave speed so much may, of course, have no desire for lowly 3.5-inch disks, which is where *VET* failed to deliver. *VET* detected all boot sectors it saw on what it considered valid disks, but failed to recognize thirteen of the samples as actually being on any sort of valid diskette, and unworthy of its attentions as a result. These are real viruses which can infect on boot-up, despite the inability of the operating system to access data stored upon the diskettes involved. This problem has been addressed before in *VB* reviews, and here prevents the attainment of a VB100% award by *Cybec*.

Curiouser and curiouser, *VET* is clearly able to scan these types of boot sector, as the on-access scanner failed to spot a completely different selection of undesirables. There was a slight slippage seen in all other categories except the Macro test-set, where full detection was achieved. This turns out to be the most common area where full scores are possible, a reassuring thought in corporate settings where macro viruses are more commonly encountered than other types. Reassuring for *Cybec* is the fact that, theoretically, their product *can* detect all viruses in *VB's* test-sets, but *VetNT* needs some reworking to do so.

Dr Solomon's AVTK v7.79 1 Dec 1997

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

Virus Bulletin's considered opinion was that the *NT* comparative would produce fewer VB 100% awards than the recent DOS equivalent. The full extent of this prediction is more significant than expected. All this is of course verbiage, for *Dr Solomon's AntiVirus Toolkit* detected everything in every set and did so both on-demand and on-access. It is the only product to receive a VB 100% award in this review.

With a speed that lies in the firmly efficient range rather than fast or slow, there is of course room for improvement if such has to be found, and a product is never really perfect until the last virus is written. Enough philosophy, roll on the next product.

EliaShim ViruSafe v2.5

ItW Overall	98.7%	Macro	98.5%
ItW Overall (o/a)	65.3%	Polymorphic	93.5%
ItW Boot	96.6%	Standard	99.4%

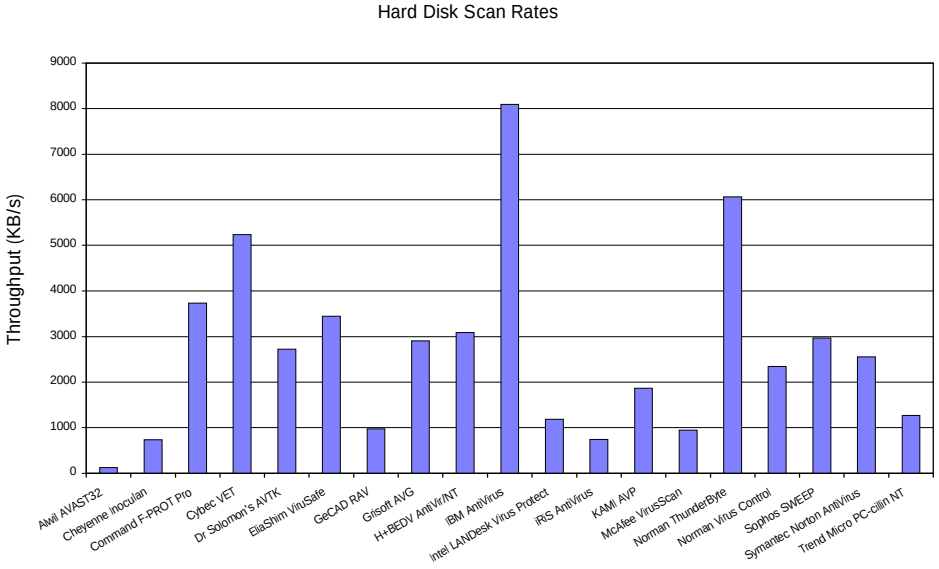
Tantalizingly close to omniscience in the on-demand tests, on the whole *ViruSafe* is the sixth consecutive product whose performance would have been seen to be remarkable two years ago. With the increasingly high expectations of the anti-virus market, and the efficiency of the engines used to meet these expectations, *EliaShim's* program is in the upper echelons, with a good few close competitors.

The detection rate has increased from its last outing, into the high nineties in all fields, and just a slight improvement will produce a few fully-detected test-sets. Boot sector detection, for example, was thrown by three variants of Hare which should be expected and detected in the future. With such jostling for the top spot, any faults are of vital importance, and *ViruSafe* falls down on false alarms. Similar to its DOS scanning, the scanner threw up twenty five cases where Cruncher-4000 was detected *in absentia*. Despite this being done in a respectable time, it is still a considerable flaw.

EliaShim is the third of this month's products to be more effective against the polymorphics when using on-access scanning. In contrast, on-access scanning does not apply to boot sectors, and changes to other categories are in the expected range of small drops in detection.

GeCAD RAV v5.20

ItW Overall	82.8%	Macro	64.3%
ItW Overall (o/a)	n/a	Polymorphic	98.1%
ItW Boot	86.5%	Standard	92.6%



GeCAD's RAV is relatively new to *VB* tests, and this is its *NT* comparative debut. It is the first, alphabetically, of six products not to include an on-access scanner. Despite its Romanian provenance, the program suffered no problems in translation, but several in implementation.

The detection rates were not high, with the exception of the Polymorphic set. 98.1% detection here places it an impressive fourth amongst some lofty company. Speed is a little on the sluggish side, and 33 false alarms are far too many.

All this accepted, the real problems came in the boot sector test, where buffering problems proved a nightmare. Each diskette was only detected as being virus-ridden once, and then not again until a different virus had been tested. Worse still, if for example, a Stoned variant was tested, it caused other successive, but different, Stoned variants to be ignored until a different family had been interpolated into the series. Somewhat disturbingly, the error message 'there is something missing please verify a:' appeared consistently during testing, and detection seemed to fail when the program was present as a tray icon. Problems there are, but promise too, and it must be remembered that some of todays high fliers made less than stunning debuts.

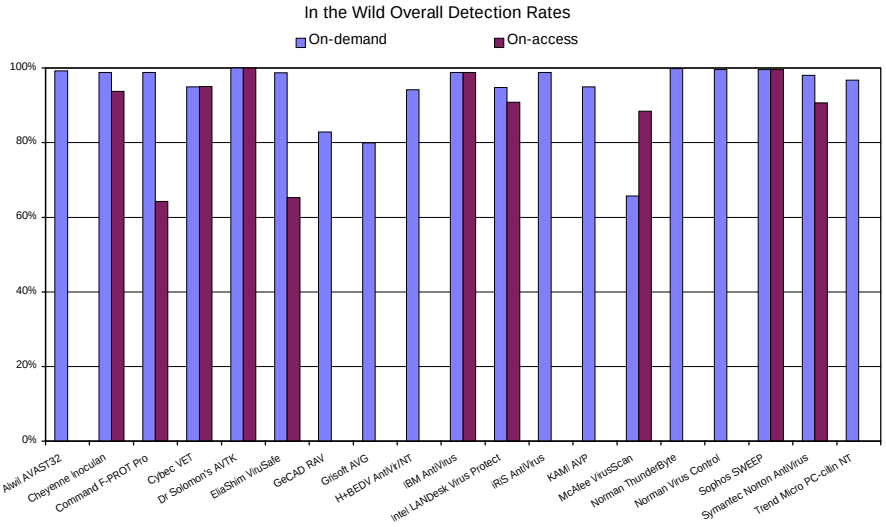
Grisoft AVG v5.0 (Build 1207)

ItW Overall	80.0%	Macro	88.3%
ItW Overall (o/a)	n/a	Polymorphic	81.6%
ItW Boot	76.4%	Standard	78.6%

Another Eastern European product relatively new to *VB* tests, *AVG* claims resident-protection for its product, which is designed to serve both *Windows 95* and *NT* equally. Some platforms are more equal than others however, and the resident-protection is in the form of a VxD – which of course does not work under *NT*. On a happier note, *AVG* saw no aberrations in the Clean test-set, which it ran through in an entirely respectable 185 seconds.

Detection rates were very similar to those seen in the DOS comparative review in the February issue, with the In the Wild Boot test-set being the particular sticking point once more. *AVG* failed to read any of those disks with less than absolutely standard formats, and thus dropped down by the unlucky thirteen into the realms of poor performance.

The detection rates in the comparative give an overview, but the standalone review on p.18 of this issue supplies a much fuller description of the nuts and bolts of the program. *AVG's* user interface is consistent across the two platforms.



not spectacular, with the expected lack of false positives. The mandatory checksumming technique meant the first run through the Clean set took 240 seconds (2225.5 KB/s).

IBMAV's on-access scanner claimed to detect viruses only in boot sectors, in memory or upon execution. This is presumably a simplification, since the on-access scanner picked up exactly the same specimens that its on-demand counterpart found. The on-access scanner does not name infections, suggesting you run the on-demand scanner instead. During testing, there was a perverse hope that the on-access scanner would detect some of the on-demand missed samples just to see the resulting confusion. Another product for whom the full set was close but not quite there.

H+BEDV AntiVirNT v5.10.01 10 Jan 1998

ItW Overall	94.2%	Macro	96.4%
ItW Overall (o/a)	n/a	Polymorphic	83.1%
ItW Boot	97.8%	Standard	96.5%

With a longer-established product than the previous pair, *H+BEDV* have yet to translate their help files into English, though menus, general instructions and icons are available in either German or English. *AntiVirNT* has no on-access scanning function. Speed-wise it kept with the pack, though five suspected viruses in the Clean set was a little disappointing. This product certainly won the 'added messages available in the clean scan' award, producing warnings of damaged files, and an over-large COM file in addition to the viruses supposedly spotted.

The CRC function in the program was not tested, leaving the usual collection of on-demand tests to contend with. The boot sector tests missed the perennial favourites of Moloch and Hare.7750, but found no trouble at all in spotting the hidden evils on the disks having possibly tricky formats. This gave a much improved set of detection figures over the September *NT* comparative, which was to a lesser extent carried over to the other test-sets. It is to be hoped that such improvement can be maintained.

IBM AntiVirus v3.02w

ItW Overall	98.8%	Macro	100.0%
ItW Overall (o/a)	98.8%	Polymorphic	96.3%
ItW Boot	97.8%	Standard	100.0%

Another big company, faring as befits its size. Against the In the Wild File set only Win95.Anxiety evaded *IBMAV*, but with two samples of Hare in the boot test this was enough to dash any hopes of 100% In the Wild detection. Polymorphics saw Cryptor.2582 the only failure, though a full set of failures admittedly, but besides these *IBMAV* detected all samples in the non-ItW test-sets. Speed was fine, though

Intel LANDesk Virus Protect v5.01 16 Dec 1997

ItW Overall	94.7%	Macro	100.0%
ItW Overall (o/a)	90.9%	Polymorphic	92.5%
ItW Boot	88.8%	Standard	97.8%

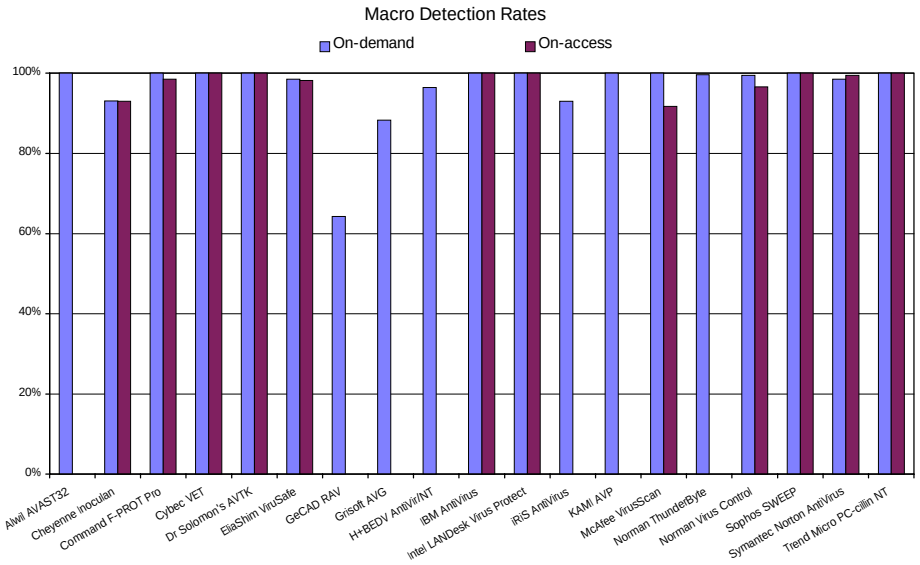
Intel suffered once more at the hands of the boot sector test. Thankfully this was simpler to discover than in some programs, multiple disk scanning being a feature more common in DOS products but supported well here. Unfortunately, *LANDesk Virus Protect* was unable to detect a selection of rather aged viruses still in the wild, again including the venerable Stoned-standard which caught it out in the previous *NT* comparative. A perfect score on the Macro test-set is encouraging, and on-demand scores against the other three test-sets were respectable but hardly earth-shattering in their magnitude.

On-access results were pretty much the same as the on-demand ones in the Macro, Polymorphic and Standard sets. In the Wild File was a little worse for on-access detection than on-demand. Similarly, the added problems with boot sectors came as no shock. Once more the errors thrown up by strange formats prevented detection of any viruses on a fair number of the samples. This took *LANDesk* to the bottom of the stack for programs with operating on-access boot scanners. As for speed, *LANDesk* is one of the more ponderous of the products, and it still manages to discover four viruses in places where they do not exist.

iRiS AntiVirus v22.03 16 Dec 1997

ItW Overall	98.8%	Macro	93.0%
ItW Overall (o/a)	n/a	Polymorphic	90.9%
ItW Boot	98.9%	Standard	99.6%

No on-access scanner here, and a display of on-demand scanning which would impress but for the better scores common in this review. At 720 seconds, *iRiS AntiVirus* required longer than average to scan the Clean test-set. Somewhat bizarrely, the program claimed that it had been altered when run, though we did not count this as a false positive to add to the two generated against the Clean set. Remembering that in the past *iRiS AntiVirus* has produced up to 139 false positives this shows a massive improvement somewhere in the code. This apart, the program operated as expected, and missed only the Hare.7610 on the boot test.



Detection rates were somewhat down from previous *Windows NT* incarnations of *iRiS AntiVirus*, though this can with hope be ascribed to the rather old scan string files submitted for testing. On a more positive note, polymorphic detection was up significantly, an area of noted weakness last September.

KAMI AVP v3.0 (Build 117) 5 Jan 1998

In the Wild Overall	94.9%	Macro	100.0%
In the Wild Overall (o/a)	n/a	Polymorphic	99.1%
In the Wild Boot	85.4%	Standard	100.0%

Rumours of great changes afoot at *KAMI* are clearly not based upon any great problems with the product as can be seen by these results. *AVP* fell well within the commonest range of speeds at 286 seconds, and threw up no false alarms, an improvement upon the previous *NT* comparative. This improvement was apparent in all facets of the detection ability of the program, which missed just one sample of DSCE.Demo in the Polymorphic test-set. The boot sector problems, on the other hand, remained much the same as before. Failure to read the thirteen confusing disks without producing errors prevented *AVP* from displaying its full ability to detect In the Wild Boot samples.

A slightly confusing artifact could also be generated if infected disks were interrupted in scanning after they had been declared infected on screen. Under these circumstances a clean disc inserted and scanned would produce a large red infected notice. With these results such niggles are not, however, a major issue.

McAfee VirusScan v3.1.4 11 Dec 1997

In the Wild Overall	65.8%	Macro	100.0%
In the Wild Overall (o/a)	88.4%	Polymorphic	98.7%
In the Wild Boot	1.1%	Standard	98.9%

McAfee VirusScan proved one of the more interesting products to test. The on-demand scanner was effective at spotting all In the Wild Files and macro viruses in the test-sets used, and put in a creditable 98.7% score in the Polymorphic set. Speed of scanning is at a rather plodding rate, but nothing was detected that should not have been. On-access the polymorphics proved rather too elusive to *VirusScan*, though detection of other file infectors was fair. This leaves the boot sector viruses. Of the 89 boot sector viruses provided, *VirusScan* detected just one on-demand. Yes, one! We were surprised too.

VB has no great wish to be sued, and so we checked this, and came to the following conclusion. ABCD, the boot virus that was detected, is on the only diskette that contains a file (a relic of an atypical replication procedure). Sure enough, if a file is placed on other boot virus test diskettes, *VirusScan* inspects the diskette properly. With no files present it returns the error 'Path A:\ does not exist' and fails to look at the boot sector.

Consider the misinformed but ubiquitous Joe Bloggs, who 'knows' that deleting all files on a disk will destroy viruses on it – if he performs this task *VirusScan* could incorrectly agree that he has been successful. This bug will also see *VirusScan* fail to detect boot infections on new, pre-formatted but infected diskettes.

At this point optimists are allowed to mention the detection rates on-access. These are a bit better, though suffering like *RAV* from a buffering problem which makes detection possible, if somewhat hit and miss. The on-access scanner is on by default, so a user would have to turn it off deliberately. In a compounding sin, however, the resident program makes scanning boot sectors an unstable affair at best. The scanner crashed *NT* to a featureless desktop no fewer than seven times in the boot sector testing process, and not on any particular subset of disks. Joe Bloggs might take this as a fair enough reason to turn off the on-access scanner – you can imagine the rest.

Norman ThunderByte v8.04 29 Dec 1997

ItW Overall	99.8%	Macro	99.6%
ItW Overall (o/a)	n/a	Polymorphic	98.1%
ItW Boot	100.0%	Standard	99.2%

After such a set of comments it takes something special to be noticed. *NTVC* can thankfully provide this however, in the amazing speed at which it scanned the Clean set. Eighty-eight seconds represents over 6 MB/s and with no false positives and without the assistance of checksumming, as used by the only faster product, is a very creditable result. In all test-sets, *NTVC* missed a smattering of samples – at the risk of being repetitive, close but no cigar.

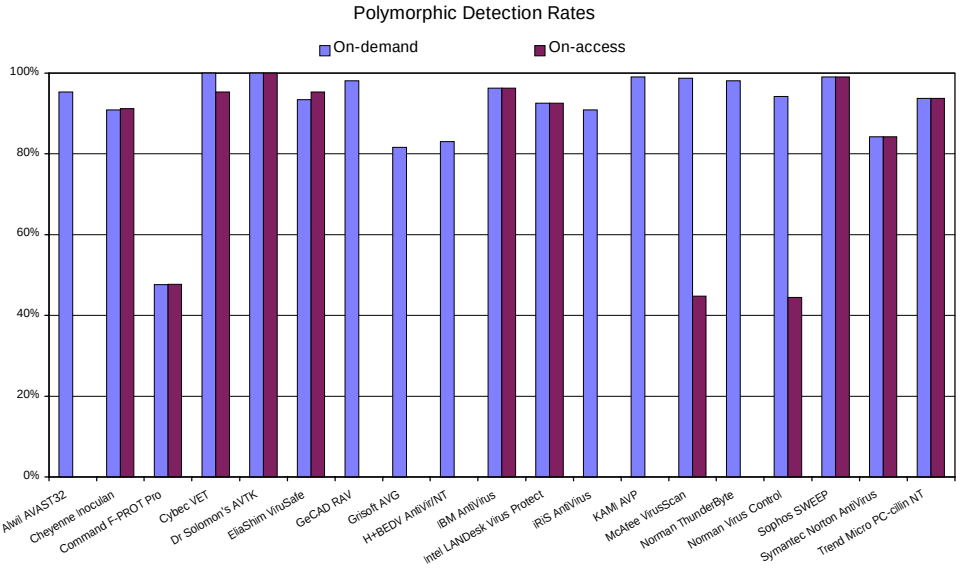
NTVC provides no on-access scanner, but instead supplies an installation checksum routine and scheduled background scanning. Neither were tested in this review.

Norman Virus Control v4.30a 5 Jan 1998

ItW Overall	99.6%	Macro	99.5%
ItW Overall (o/a)	n/a	Polymorphic	94.2%
ItW Boot	100.0%	Standard	99.7%

The last false alarm reared its head in a middle-ranking speed test from *NVC*. On-demand, *NVC* is efficient but failed to deliver the raft of 100% results we have seen from its brethren in recent comparatives. Responsibility for this is entirely attributable to its failure to detect all eighteen samples of Morphine.3500. Polymorphics were also less comprehensively detected than is ideal, despite improving considerably over the last three months.

Testing *NVC's* interesting approach to on-access virus protection, involving behaviour blockers and other mechanisms, is beyond the scope of this review. The only 'traditional' on-access scanner is the macro detector, Cat's Claw.



This component did not quite detect as many macro viruses as the on-demand scanner. Logging of on-access scanning was less controllable than suggested. This proved a common flaw in the tested programs, too many of which, on-access, relied upon binary log files, or provided no log file.

Sophos SWEEP v3.05 5 Jan 1998

ItW Overall	99.6%	Macro	100.0%
ItW Overall (o/a)	99.6%	Polymorphic	99.0%
ItW Boot	100.0%	Standard	99.7%

A good result for *Sophos*, but a definite downturn from past near-perfect detection. *SWEEP* missed the new ItW File virus Win95.Anxiety and, mysteriously, five samples of Neuroquila.A from the Polymorphic test-set. The latter is surprising given that *SWEEP* has consistently detected all samples in this test-set for many reviews. In the Standard set Positron was undetected, which is almost certainly by design as it has been the lone, missed sample from the Standard test-set for several consecutive comparatives.

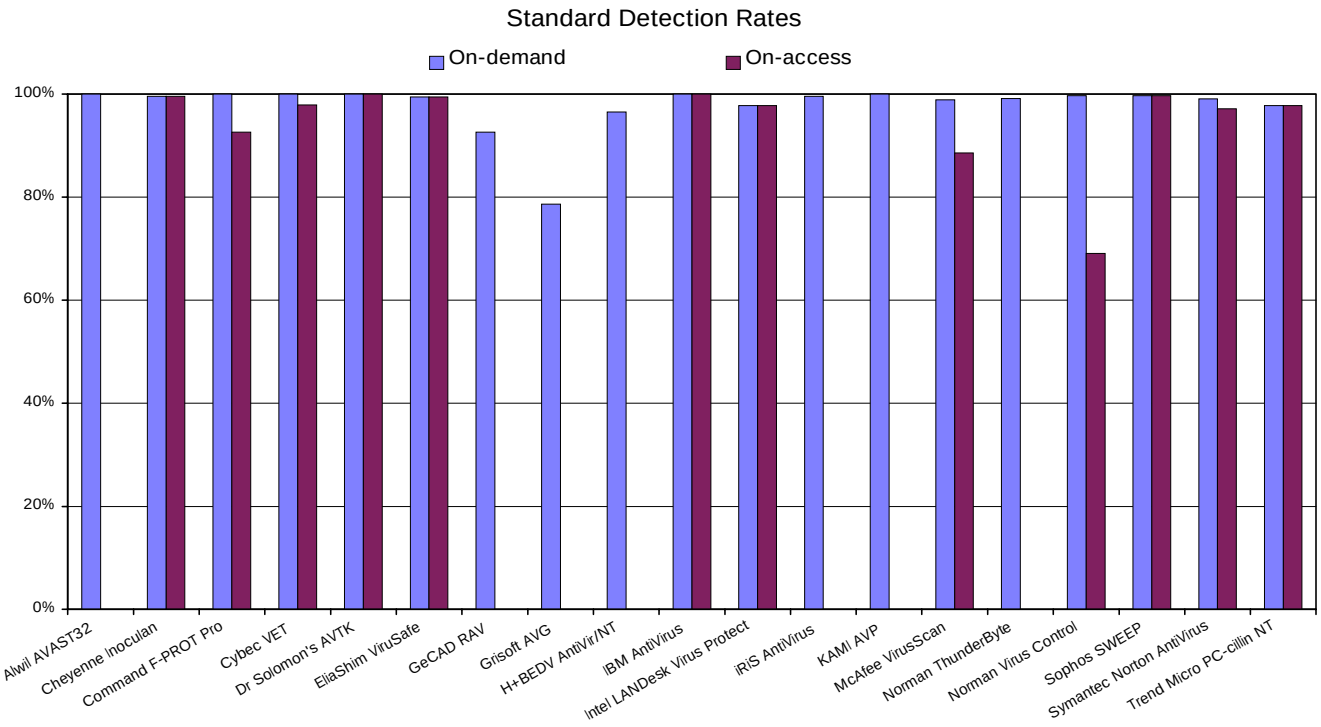
SWEEP's on-access component proved the only equal to *Dr Solomon's* in detecting all boot sector viruses, and like *AVTK* and *IBM AntiVirus* the results obtained by on-access and on-demand scanning were exactly comparable. Speed on-demand was neither good nor bad, and the clean files were all correctly reported as uninfected.

Symantec Norton AntiVirus v4.0

ItW Overall	98.1%	Macro	98.5%
ItW Overall (o/a)	90.7%	Polymorphic	84.3%
ItW Boot	100.0%	Standard	99.1%

NAV's discovery of all samples in the on-demand boot test continues its good, recent record there. Detection of Standard test-set viruses has improved, yet in other on-demand areas the new specimens proved problematic for *NAV*. No false positives were produced on the other hand. Scanning speed was decidedly average.

Worse news was in evidence with the on-access boot tests, where a combination of simple misses and inability to access diskettes gave rise to nineteen misses. As an addition to these imperfections, the buffering syndrome similar to that seen with *GeCAD RAV* and *McAfee VirusScan* was again apparent. Results other than these were comparable to those of the on-demand tests.



Trend Micro PC-cillin NT v1.0 VPN 347

ItW Overall	96.8%	Macro	100.0%
ItW Overall (o/a)	n/a	Polymorphic	93.8%
ItW Boot	94.4%	Standard	97.8%

Trend's PC-cillin NT suffers a little by being at the end of the alphabetical trail, where it nevertheless manages to raise some points not yet addressed. On-demand Macro detection was a perfect 100%. The three Hare variants, Moloch and Neuroquila.A were the only misses in the on-demand Boot sector test. Though the scan speed is slower than average, it was by no means frustratingly so, and threw up no false positives. *PC-cillin's* other on-demand results were unexceptional by dint of resembling those of other products.

The on-access scanner does not test for boot viruses, but all other test-sets were detected equally well on-access and on-demand. Given how few products detected (and missed) the same viruses in on-access as in on-demand modes, this is actually an encouraging result, in terms of what it says about the product's developmental consistency.

Conclusion

A comparison with last month's DOS comparative shows, perhaps not surprisingly, that *NT* products handle macro scanning more effectively than their DOS-based brethren. Unfortunately, it appears that the macro detection gains are the roundabouts to the boot virus swings.

This is our third *Windows NT* comparative and this is the third time we have shown the general inadequacy of certain approaches to dealing with boot sector viruses under this operating system. Although supplanted as commonest by some macro viruses, boot viruses still account for a significant slice of infections reported in our monthly Prevalence Tables. Moreover, we still receive many panicked reports of infected systems – clearly many users are still not using the common, BIOS-based against protections. Thus, reliable detection of these viruses is still important. We hope to not have to repeat this complaint in the next *NT* comparative.

An interesting feature of the current results is how the recent appearance of Win95.Anxiety and its relatively rapid appearrance in the WildList had such a major influence on the ItW File detection results. Although not necessarily the sole malefactor, it was missed by ten of the products tested, and was the single detractor from a perfect ItW File score for two products, denying one of them a VB 100% award. Another new entrant to the ItW File set, which also acted as a spoiler for many, was Morphine.3500, again contributing to the collapse of ten products' VB 100% hopes.

Congratulations to the *Dr Solomon's* team for their second consecutive perfect score across the board.

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 test-sets were held in a read-only directory on the server. 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-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/199803/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

PRODUCT REVIEW 1

AVG v5.0 for Windows 95

Dr Keith Jackson

Czech developers *Grisoft* claim that *AVG* is 'a sophisticated antivirus system for detecting and removing viruses'. The product can operate under DOS, *Windows 3.1*, *Windows 95* and *NT*, or across a network. However, this review only covers the standalone *Windows 95* version.

Installation

AVG was provided for review on three 3.5-inch, 1.44 MB floppy disks. In fact, two identical sets of disks were provided – I know not why.

Installation was initiated by executing SETUP.EXE. After reading warnings about the licensing conditions, I had to enter my name, a company name, and the program serial number before installation could proceed. The name of the subdirectory where *AVG's* files were to be stored could be altered if required, and an option was provided to install *AVG's* memory-resident component. The usual bargraphs whirred, the other floppy disks were requested, and a reboot was performed. All in all a painless program installation, much as we have come to expect.

Documentation

AVG arrived with three small A5 books entitled 'Installation and First Steps', 'User Manual', and 'Computer Viruses and You'. The titles are fairly self-explanatory. The 'Installation' booklet is very short and to the point. It contains just over eight pages, nearly half of which are taken up with the licence conditions and details of the warranty. This manual can be succinctly summarized thus: use the floppy disks, follow the instructions to install the *AVG* software, and do not forget to read the licence conditions (or else…).

Speaking of the *AVG* licence, it contains some very odd clauses; for instance, the product is not sold, it is licensed for a period of time, which is fairly standard. However, all parts of the packaging must be kept for when the licence expires, which is presumably when you no longer require the product and stop paying for upgrades. The licence explicitly includes 'the wrapping of the distribution package' in the list of things that must be retained for subsequent return to the vendors.

Lawyers are wonderful – just when you thought that they might inhabit the real world after all, they come up with nonsense like that and shatter the illusion. Hands up all those users who not only keep the box in which a software product is packed, but also keep the wrapping paper. Nobody? I thought so.

The licence also includes a wonderful cop-out which states that (and I quote) 'The manufacturer does not guarantee the perfect operation of the system if the system is used on equipment not 100% compatible with a standard IBM PC'. Note that no attempt is made to define a 'standard IBM PC'. Nor could it be, such a beast no longer exists – if it ever did. When things get rough any half-decent lawyer has enough in that one phrase to defend the developers of *AVG* against anything. Absolutely anything.

The User Manual is well written, but suffers somewhat because it applies to several versions of *AVG*, running under various operating systems. This inevitably makes it vague on detail. Still, given that many (most?) anti-virus vendors seem to have given up on manuals completely, at least *AVG* provides something in printed form.

'Computer Viruses and You' a slim, A5 volume, contains a good description of computer viruses, how they operate, their history, and the parts of the PC that they attack. It would be especially easy for a first-time user to follow the explanations provided.

Interface

In last month's review I complained that all *Windows 95* anti-virus software looked the same. No sooner had the words tripped off my keyboard and into print, than something comes along that looks completely different.

Down the left hand side of *AVG's* main window a list of section headings is provided ('Tests', 'Utilities', 'Help' etc). Each of these headings can be expanded (by double clicking on it) to reveal the options available within that section. Once an action has been selected, activity takes place in the main part of the window, while there are

AVG's user interface breaks the mould somewhat, but is an eminently usable design.

several large buttons across the bottom edge. It is refreshingly different from the usual drop-down *Windows* menus, and it works rather well.

Heuristics

A short excursion into *AVG's* heuristic capability is called for at this point. One of the main components in *AVG's* armoury is its 'Complete Test'. This option scans everything, using both an ordinary scanner and a heuristic scanner. If *AVG* is sure that a particular file is 'clean', it adds it to the 'validation database'. Future 'Complete Test' activations need only scan files whose checksums have changed since the database entry was created, with a consequent reduction in scan time. *IBM's* scanner uses the same tactic.

So far, so good. However, the *AVG* documentation warns that the heuristic scanner can produce false alarms, and sure enough it does. Before installing *AVG*, I re-installed *Windows 95* on my test PC. Therefore, the only files on the C drive were either from *Windows 95*, or they were installed by *AVG*. The first time I requested a 'Complete Test', *AVG* found that three of the *Windows 95* files were infected, two by an unknown virus. More worryingly, one file was thought to be infected by the 'LSD' virus.

The first 'Complete Test' execution took 1 minute and 2 seconds to execute, having tested 800 'objects' (their word). The second and subsequent executions took just 22 seconds to complete, with the same three COM files found to be infected.

Scanning

I tested *AVG's* detection capabilities against the *VB* test-sets (see the 'Technical Details' section below) which are stored on CD-ROM. The *AVG* scanner stated that it detected 514 of the 549 samples contained in the In the Wild test-set (93.6%). Frankly, this figure is disappointing; it should be closer to 100%. When the heuristic scanner was used, the detection rate increased to 95.6%, or 525 of the ItW test files. This was better, but still nowhere near 100%, which belied many of the claims made for the efficacy of the heuristic scanner. Heuristic detection still had one trick up its sleeve – a 'sensitive' mode of operation, but this did not increase the number of viruses detected.

However, the above result was better than the 536 out of a possible 774 viruses (69.2%) that the *AVG* scanner detected against the Standard test-set. Once again the heuristic scanner improved things somewhat, but it only raised the number to 713 (92.1%) when the 'default' heuristic was used ('sensitive' heuristic detection obtained exactly the same result).

When the 716 files of the Macro test-set were scanned, no matter which method of scanning or what type of heuristic scanning was used, the result was always the same – 650 were detected as being infected (90.7%), i.e. heuristic detection does not increase the chance of detecting a macro virus. This is perhaps unsurprising, and many products exhibit exactly the same property.

The Polymorphic test-set contains 13,000 viruses (500 samples of 26 viruses), and the *AVG* standalone scanner detected 10,526 (80.9%). Heuristic detection fared better, raising the detection rate to 11,996 (92.2%). This result remained the same no matter whether 'default', or 'sensitive' heuristic detection was used.

In the Wild Boot sector virus detection was a little better at 94.5% (86 from 91), but this is a test where you should expect 100% detection.

False Alarms

When I tested *AVG* against the *VB* Clean test-set (5500 executable files held on CD-ROM, all of which have been copied from well-known software products, none of which are infected with a virus), it did not find any virus infections. Given that *AVG* had informed me that three *Windows 95* files were infected (see above), this result seemed rather curious.

Speed

Using its default settings, *AVG* scanned the C: drive of my test PC in 20.9 seconds. It is interesting, and highly confusing, that this is actually faster than the 22 seconds quoted above for a 'Complete Test' during which only the files that have been altered are actually scanned. What is the point in having the 'Complete Test' inspect its validation database if this process is slower than actually scanning the files? Most odd.

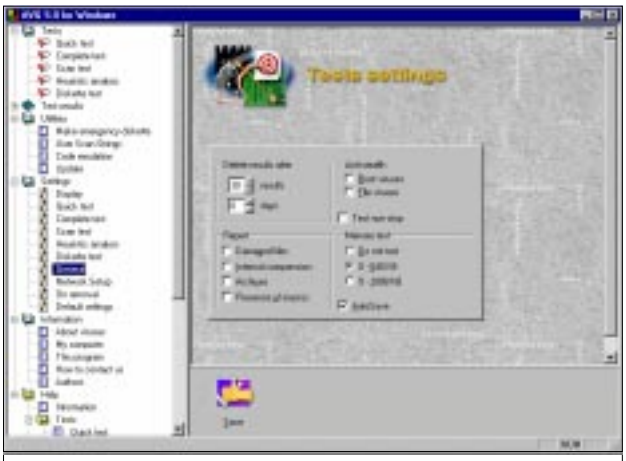
I scanned inside internally compressed files (the scan time went up to 23.6 seconds), and inside archive files (ZIP, ARJ etc.), which further increased it to 28.3 seconds. Finally, I used the heuristic scanner, and this pushed the scan time to 51.1 seconds.

For comparison purposes, the DOS version of *Dr. Solomon's Anti-Virus Toolkit* took 57 seconds, and the DOS version of *SWEEP* from *Sophos* 48 seconds, to perform the same scan. *AVG* is no slowcoach, it whizzes along much faster than competitor products on the market.

Memory-resident Scanning

The memory-resident scanner provided with *AVG* can be set up to check floppy disks or files and to ask the user what to do if an infection is found. Note that I have not mentioned any options that can tailor how this software actually operates – there do not appear to be any.

The control program for the memory-resident software still has a few obvious bugs. Click the 'schedule' tab and the program closes. This is not exactly an endearing habit. Likewise, the boxes that activate scanning of floppy disks and/or files can be activated from almost anywhere along a



The general settings page is one of the many pages of configuration options.

horizontal line stretching out from the box itself, through its title, and on towards the right-hand side of the window. The invoice for my consultancy fee is in the post!

AVG's memory-resident scanner checks for viruses while infected files are being copied from one location to another. It seemed reasonable at detection, although absolute figures are hard to come by as it always interrupted a file copy whenever an infected file was found.

I waded through hundreds of individual keypresses for the ItW test-set, only to find that after 248 viruses had been detected, the screen informing me of a virus detection was replaced by a series of apparently randomly-coloured rectangles. This is called a software bug.

As expected, the memory-resident software was far less efficient at spotting polymorphic test samples. Indeed, it had got about one third of the way through copying the entire 13,000-strong Polymorphic test-set before it detected a single file as being infected.

When I tried to delete files that had been used in this copying test, the memory-resident software indicated files that were in the *Windows* Recycling Bin as infected. This may be thorough, but it is also a thorough nuisance. There should be an option available to disable this action.

The Rest

A 'Quick Test' can be executed which just looks at the disk locations and files that are deemed to be either important, or likely to be infected. This list can be tailored by the user. Using its default settings the 'Quick Test' option checked the C: drive of my test PC in about one second, almost too quick to measure. It really lives up to its name!

A specific menu option is provided to check out floppy disks. I like this idea – many a time I have wrestled with a product's intricate menu system trying to find out how to scan a floppy disk. Having an easy way to kick-start this process is a real boon.

On-line information about viruses, and families of viruses, is provided. What is there is very helpful, easy to understand, and most comprehensive. However, there are about 170 names of individual viruses in the list entitled 'Virus Information'. Some of these contain more than one entry, but even so this does not even begin to compare with the total of well over 10,000 viruses of which many scanners claim knowledge.

Finally, utilities are included to make an emergency diskette, introduce scan strings entered by the user, update the software, and run something called 'Code Emulation'. This last facility allows 'expert' (*Grisoft's* word) users to analyse suspicious programs by stepping through their code with the emulator from the *AVG* heuristic engine – not for the faint-hearted this one.

Conclusion

Face facts – the basic detection rate of *AVG* needs some more work. Competitor products are much better at the core task of detecting viruses. Having said that, the operational aspects of *AVG* are good, it is a delight to use, works very quickly indeed, and provides all the usual features.

The developers of *AVG* are probably perfectly well aware of these conclusions; they must know their current 'hit rate'. It is obvious in their own 'Virus Information' section, which is somewhat short on content. The question is – are they prepared to put in the sheer number of man hours that are required to increase the virus knowledge incorporated into *AVG*? We shall see.

Do not even consider purchasing *AVG* unless the developers agree to remove the 'standard IBM PC' clause from their licence. It is onerous and makes it impossible *ever* to have a legal claim against the developers. Likewise, unless you have a fetish for collecting waste paper, insist that the clause about keeping the product's wrapping paper for ever and a day is removed from the *AVG* licence – it is just daft.

Technical Details

Product: *AVG v5.0 for Windows 95*.

Developer: *Grisoft Software Ltd*., Lidicka 81, 602 00 Brno, Czech Republic, Tel +420 5 4124 3865, fax +420 5 4121 1432, BBS +420 5 4124 3858, email: grisoft@grisoft.anet.cz, WWW http://www.grisoft.com/.

Availability: *AVG* requires at least 5 MB of hard disk space.

Version evaluated: 5.0P, build number 1207, resident VxD driver version 1.7.

Serial number: 50U-1-102955-MVJ.

Price: Licence price for single user $49, with a sliding scale to $30 per licence for 51 to 100 users. Large volume discounts can be negotiated with the vendor.

Hardware used: A 133 MHz Pentium with 16 MB of RAM, a 3.5-inch floppy disk drive, a CD-ROM drive, and a 1.2 GB hard disk divided into drive C (315 MB), and drive D (965 MB). This PC can be configured to run *Windows 95*, *Windows 3.11*, *Windows 3.1*, or DOS 6.22.

Test-sets: See *VB*, September 1997, p.16.