# COMPARATIVE REVIEW

## Any ImprovemeNT?

Six months, an English summer and much Internet Worm excitement have passed since the last *NT* comparative, back in March of this year. Then it was eighteen products that were submitted for review. Sixteen are present this time.

### Test Procedures

As usual for the *VB* comparatives, three essentially identical test machines were used for the product testing. The hard drives of each were completely wiped with a fresh *NT 4.0* (SP 5) image prior to the testing of each product. To eliminate any potential discrepancies, all speed tests (scan rates and scanner overheads) were performed upon one of the machines, whilst disconnected from any network.

The test-sets were updated from those used in the previous comparative, and importantly, the In the Wild (ItW) File and Boot sets were aligned to the June 1999 WildList. New additions to the ItW viruses included W97M/Pri.A, W97M/Walker.E, W97M/Walker.F, and the email propagating Win32/ExploreZip and Win32/PrettyPark Worms. The COM/EXE infecting ACG.B joins ACG.A in the Polymorphic set, and the Macro set welcomes W97M/ZMK.P, the B, C and D variants of W97M/Lys, and W97M/Melissa.I amongst others. Additionally, samples infected with {W95,W97M}/Heathen.A, a virus capable of infecting both *Windows* executables and *Word* documents, have been added to the Standard and Macro test-sets. For a complete listing of the viruses in each of the test-sets, see the URL quoted at the end of this review.

Speed tests were performed in order to assess two aspects of each of the products. Firstly, the overhead of each of the on-access scanners was assessed, by measuring the time taken to copy a set of 100 executable and 100 OLE2 files between directories, with the on-access scanner in a variety of configurations. For presentation in this review, the results have been normalized with respect to a common baseline of 17 seconds, enabling them to be presented in units of time. Next, the scanning speed of the on-demand scanners were measured, by timing how long it took to scan a set of 5,500 COM and EXE executables (520 MB), and a set of 373 OLE2 files (65.3 MB). These latter tests double up as false positive tests, since all the files are clean and no viruses should be detected.

On-demand tests were performed whilst logged in as Administrator on the workstation. The test-sets were stored on a network drive as a read-only share. For products that were incapable of scanning network drives, the test-set was copied to a local hard drive. On-access detection rates were determined with the usual *VB* method – using a utility that recursively searches the test-set directory tree, attempting to open each of the files encountered. For scanners where the option to 'deny access' to suspected files was unavailable, the configuration was altered to scan on file writes, and delete infected files. Subsequently, the test-set was copied to a local hard drive. In some cases it was necessary to copy the test-set repeatedly between different directories on the hard drive until no further infections were found. This latter testing method was also applicable to products that could only scan on file writes.

Full details of the results are presented in the main tables. The brief results summary presented under each of the product headings are those for on-demand scanning unless otherwise indicated.

### Alwil Avast32 v3.0-154 (24/6/99)

| | | | |
|---|---|---|---|
| ItW Overall | 99.7% | Macro | 95.3% |
| ItW Overall (o/a) | 98.2% | Standard | 98.4% |
| ItW File | 99.7% | Polymorphic | 93.9% |

Since its last appearance, *Avast32* has received a fair amount of attention from its developers at *Alwil*. As with many of the other products, files of *PowerPoint* format are now supported, as is scanning within ZIP archives.

On-demand detection rates are respectably high – only the failure to detect one of the three Win95/Kenston samples prevented *Avast32* from claiming the VB 100% award. A variety of samples were missed from the other test-sets – a handful of Marburg-infected executables, the polymorphic X97M/Soldier.A, and the {W32, W97M}/Heathen.A samples, a recent addition to the test-set.

*VB* has been unable to test the on-access scanner of *Avast32* in previous tests, due to its dependence upon file execution. This latest version scans on file *writes* however, and so for the first time, the standard of *Avast32's* real-time protection has been assessed. Detection rates were determined by copying the test-set to the local hard drive with the scanner set to delete infected files. The copied files were then copied between directories on the local hard drive, until after three iterations of the process, no further infections were found. On the whole, detection rates were lower than those observed during on-demand scanning.

Testing on-access scanning of the ItW boot viruses proved wearing. As with other products in this and previous comparatives, *Avast32* failed to detect disk changes reliably. Detection (or not) also seemed to depend upon the sequence in which the test disks were checked. Admittedly, bombarding a scanner with a large number of diskettes infected with different boot viruses may not be a *realistic* scenario, but these observations do reveal a slight weakness in the on-access scanner's architecture.

| On-demand tests | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | % | Missed | % | Missed | % | Missed | % |
| Alwil Avast32 | 0 | 100.0% | 1 | 99.7% | 99.7% | 142 | 95.3% | 273 | 93.9% | 22 | 98.4% |
| CA InnoculateIT | 0 | 100.0% | 0 | 100.0% | 100.0% | 7 | 99.7% | 174 | 96.9% | 1 | 99.9% |
| CA Vet Anti-Virus | 0 | 100.0% | 0 | 100.0% | 100.0% | 22 | 99.4% | 268 | 93.9% | 3 | 99.7% |
| Command AntiVirus | 0 | 100.0% | 2 | 99.4% | 99.4% | 14 | 99.8% | 112 | 98.0% | 0 | 100.0% |
| Data Fellows FSAV | 0 | 100.0% | 4 | 99.7% | 99.7% | 20 | 99.4% | 16 | 99.7% | 0 | 100.0% |
| Dialogue Science DrWeb32 | 0 | 100.0% | 2 | 99.1% | 99.1% | 18 | 99.3% | 10 | 99.8% | 1 | 99.7% |
| Eset NOD32 | 0 | 100.0% | 0 | 100.0% | 100.0% | 7 | 99.7% | 0 | 100.0% | 1 | 99.7% |
| GeCAD RAV | 0 | 100.0% | 0 | 100.0% | 100.0% | 25 | 99.1% | 503 | 96.9% | 82 | 94.3% |
| Grisoft AVG | 0 | 100.0% | 3 | 99.1% | 99.1% | 55 | 98.3% | 96 | 96.8% | 32 | 98.6% |
| Kaspersky Lab AVP | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | 0 | 100.0% | 0 | 100.0% |
| NAI VirusScan | 0 | 100.0% | 1 | 99.9% | 99.9% | 3 | 99.9% | 0 | 100.0% | 0 | 100.0% |
| Norman Virus Control | 0 | 100.0% | 0 | 100.0% | 100.0% | 5 | 99.8% | 174 | 96.9% | 0 | 100.0% |
| Proland Protector Plus | 3 | 91.8% | 81 | 89.2% | 89.4% | 1104 | 62.8% | 11138 | 22.1% | 515 | 65.2% |
| Sophos Anti-Virus | 0 | 100.0% | 9 | 97.9% | 98.1% | 53 | 98.2% | 174 | 96.9% | 12 | 99.5% |
| Stiller Integrity Master | 0 | 100.0% | 201 | 64.5% | 66.7% | 1555 | 50.2% | 10143 | 29.8% | 255 | 83.9% |
| Symantec Norton AntiVirus | 1 | 97.3% | 0 | 100.0% | 99.8% | 14 | 99.4% | 264 | 93.9% | 1 | 99.7% |

## CA InnoculateIT v4.53 (24/6/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 99.7% |
| ItW Overall (o/a) | 98.6% | Standard | 99.9% |
| ItW File | 100.0% | Polymorphic | 96.9% |

Now the proud owners of *Cybec's Vet Anti-Virus*, it will be interesting to monitor how *Computer Associates* develops its two anti-virus siblings. Despite being obviously different products, confusion between the two will almost certainly exist, especially since the *Innoculate IT Personal Edition* that is available for free download from the *CA* site, is in fact, the *Vet* product in disguise. The product reviewed here is the *Enterprise Edition*, that native to *CA*.

*InnoculateIT*, has put in some solid performances over recent comparatives – its only downfall has been its stability. Thankfully, during testing of this version of the product no serious stability problems were encountered. However, testing the overhead of the on-access scanner proved problematic when it was set to scan incoming files. The usual *VB* method of measuring overhead was employed, which, for most products, returns very similar times for each iteration of the copying process. With *InnoculateIT* however, the times were extremely erratic, and it was not possible to obtain a consistent set of times. The results quoted are therefore an average of all the times recorded.

Detection-wise, the product maintains the high standards it has set previously, attaining the VB 100% award again. Results were poorer across all the test-sets during on-access scanning, due partly to the failure to check sufficient file types. This was most in evidence in the ItW and Polymorphic sets, where screen saver (SCR) samples infected with Marburg and TPVO.3783.A slipped through the net.

## CA Vet Anti-Virus v10.0.2 (2/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 99.4% |
| ItW Overall (o/a) | 99.8% | Standard | 99.7% |
| ItW File | 100.0% | Polymorphic | 93.9% |

When commencing the testing of some of the products submitted to *VB*, there is often a feeling of apprehension, as a multitude of potential problems are anticipated. Not so, with


*Vet Anti-Virus*. *Vet* has always been second to none in terms of stability, and, clearly, its detection capabilities are equally competitive. It was in September 1998 that *Vet* last earned the VB 100% award, and so perhaps it is fitting that a year on, it achieves that status again.

Interestingly, four Marburg samples were missed from the Polymorphic test-set during both on-demand and on-access scanning. As with the majority of the products, detection rates were generally lower during on-access scanning, where, in this case, O97M/Tristate.C infected *PowerPoint* samples were missed from the ItW set.

## Command AntiVirus v4.57β (1/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 99.4% | Macro | 99.8% |
| ItW Overall (o/a) | 98.8% | Standard | 100.0% |
| ItW File | 99.4% | Polymorphic | 98.0% |

Failure to detect two of the three samples of Pieck.4444.A in the ItW set kept the VB 100% award at arm's length from *Command Software AntiVirus* (*CSAV*).

Elsewhere, detection rates were high. In the Polymorphic set, the bulk of the misses were due to only a third of the ACG.A samples being detected. In the Macro set, all the samples infected with the polymorphic X97M/Soldier were missed, as was one of the three PP97M/Vic.A samples.

*CSAV's* performance in the speed tests was fairly average, giving a throughput of approximately 1400 and 2300 KB/s for scanning executable and OLE2 files respectively. The *Dynamic Virus Protection* (*DVP*) facility that is the on-access scanner of *CSAV* induced a reasonably large overhead of just over 220% when enabled.

## Data Fellows F-Secure Anti-Virus v4.04

| | | | |
|---|---|---|---|
| ItW Overall | 99.7% | Macro | 99.4% |
| ItW Overall (o/a) | 99.2% | Standard | 100.0% |
| ItW File | 99.7% | Polymorphic | 99.7% |

*Data Fellows F-Secure Anti-Virus* (*FSAV*) keeps up the high standard of detection set by the other products so far in this review. Failure to cope successfully with *PowerPoint* file formats resulted in missing all the samples infected with the A, B, C and D variants of O97M/Tristate, PP97M/Vic.A and PP97M/Shaper.A, for both on-demand and on-access scanning. A handful of ACG.A samples was also missed from the Polymorphic set.

Results were slightly poorer for on-access scanning, due mainly to missing the VxD samples of Win95/Fono, Win95/Navrhar and Win32/PrettyPark.

As ever, the use of two detection engines in the one product gives the expected results – high detection rates but only a mediocre scanning speed. This was also reflected in the overhead of the real-time monitor, *GateKeeper*, which at 225% was slightly above the average observed across the products. One or other of the detection engines could be removed from *FSAV*, although whether such a sacrifice to the detection capabilities would be worth it in terms of scanning speed is doubtful.

| On-access tests | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | % | Number | % | Number | % | Number | % |
| Alwil Avast32 | 3 | 91.8% | 7 | 98.6% | 98.2% | 146 | 95.3% | 311 | 92.9% | 8 | 99.5% |
| CA InnoculateIT | 3 | 91.8% | 16 | 99.0% | 98.6% | 36 | 98.9% | 420 | 95.9% | 1 | 99.9% |
| CA Vet Anti-Virus | 0 | 100.0% | 3 | 99.7% | 99.8% | 38 | 98.9% | 768 | 90.8% | 6 | 99.5% |
| Command AntiVirus | 3 | 91.8% | 3 | 99.3% | 98.8% | 17 | 99.7% | 112 | 98.0% | 0 | 100.0% |
| Data Fellows FSAV | 0 | 100.0% | 6 | 99.1% | 99.2% | 28 | 99.1% | 23 | 99.6% | 9 | 99.7% |
| Eset NOD32 | 0 | 100.0% | 0 | 100.0% | 100.0% | 7 | 99.7% | 2 | 99.9% | 1 | 99.7% |
| GeCAD RAV | n/a | n/a | 0 | 100.0% | n/a | 13 | 99.5% | 503 | 96.9% | 82 | 94.3% |
| Grisoft AVG | 0 | 100.0% | 4 | 99.0% | 99.1% | 61 | 98.2% | 268 | 93.9% | 112 | 91.6% |
| Kaspersky Lab AVP | 0 | 100.0% | 0 | 100.0% | 100.0% | 0 | 100.0% | 0 | 100.0% | 0 | 100.0% |
| NAI VirusScan | 0 | 100.0% | 1 | 99.9% | 99.9% | 3 | 99.9% | 0 | 100.0% | 0 | 100.0% |
| Norman Virus Control | 3 | 91.8% | 7 | 99.4% | 99.0% | 50 | 98.6% | 177 | 96.7% | 0 | 100.0% |
| Sophos Anti-Virus | 0 | 100.0% | 8 | 98.0% | 98.1% | 52 | 98.2% | 174 | 96.9% | 12 | 99.5% |
| Symantec Norton AntiVirus | 1 | 97.3% | 0 | 100.0% | 99.8% | 14 | 99.4% | 264 | 93.9% | 1 | 99.7% |

## Dialogue Science DrWeb32 v4.11 (2/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 99.1% | Macro | 99.3% |
| ItW Overall (o/a) | n/a | Standard | 99.7% |
| ItW File | 99.1% | Polymorphic | 99.8% |

Processing the variety of log files produced by sixteen different products is a task enough by itself. Generally, problems exist with products that use multiple tags within the same log to mark infected files. However, *DrWeb32* introduced a new dimension to the task by logging certain scanned files as both clean and infected!

This slight inconvenience aside, *DrWeb32* achieved high detection rates across all the test-sets, although failing to detect Win95/PrettyPark cost the Russian product the VB 100% award.

Currently *DrWeb32* does not incorporate an on-access scanner, an issue which is currently being addressed by the developers. Come the next comparative, when on-access scanning is incorporated into the VB 100% award, the performance of this component will be of much interest.

## Eset NOD32 v1.20 (2/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 99.7% |
| ItW Overall (o/a) | 100.0% | Standard | 99.7% |
| ItW File | 100.0% | Polymorphic | 100.0% |

Another product proving straightforward to test was this Slovak offering. An anti-virus product in the strictest sense of the term, not jam-packed with additional features, *NOD32* does what it claims extremely well. Only eight and ten samples were missed across all the test-sets during on-demand and on-access scanning respectively.

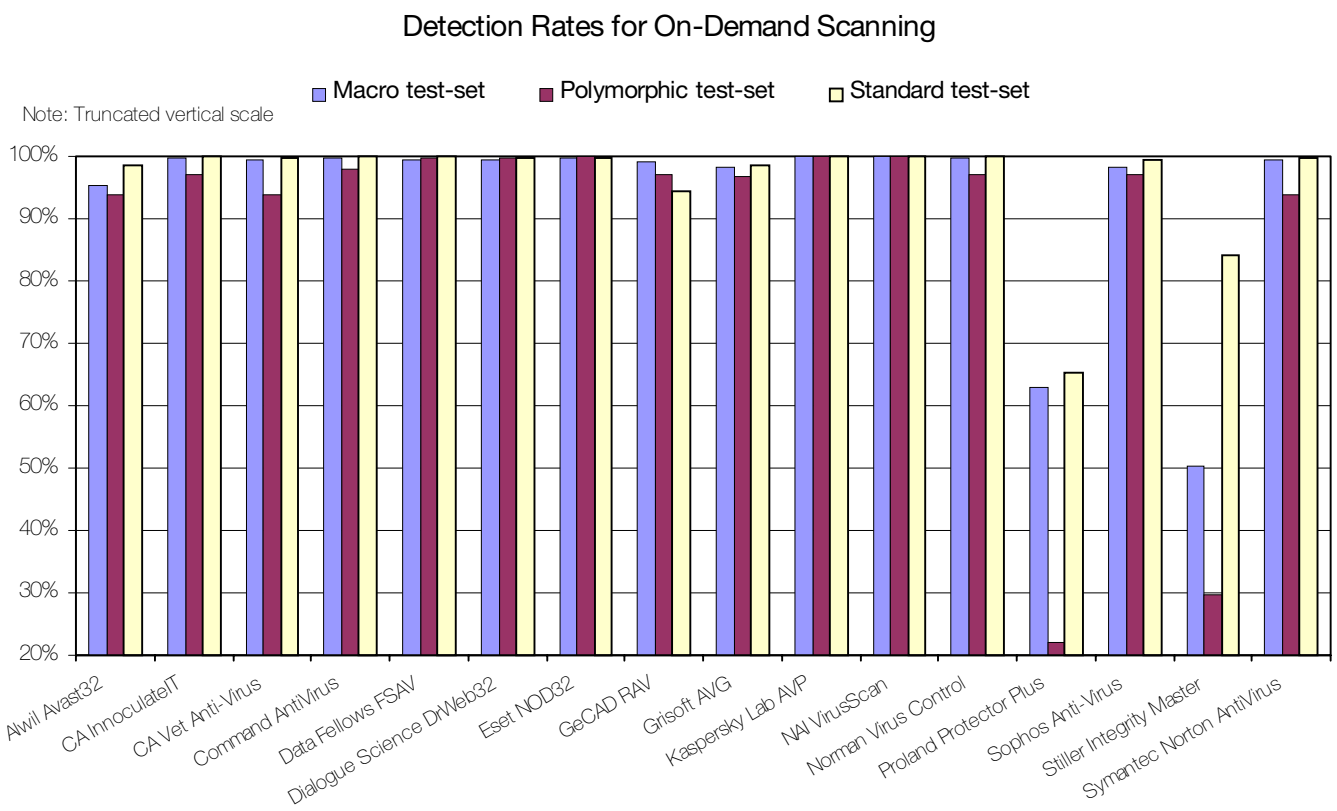
These misses were registered against samples infected with {Win95/W97M}/Heathen.A, and document templates infected with the B, C and D variants of W97M/Lys. Two samples of the polymorphic Nightfall.4518.B were also missed by the on-access scanner.

## GeCAD RAV v7.0 (2/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 99.1% |
| ItW Overall (o/a) | n/a | Standard | 94.3% |
| ItW File | 100.0% | Polymorphic | 96.9% |

The recipient of a major facelift quite recently, *RAV 7* is the first of *GeCAD's Romanian Anti-Virus* products to sport an on-access scanner. Such a feature is pretty much essential for any product vying for attention in the anti-virus arena today.

Achieving complete detection of the ItW file collection in both on-demand and on-access scanning will certainly please the developers. Unfortunately, on-access scanning of




floppy boot sectors was not supported in the submitted version of *RAV*, and so overall ItW detection of the on-access scanner can not be assessed. *VB* has been informed that plans are currently afoot to address this deficiency.

Outside of the ItW sets, detection rates were not as high as some of the other products. Failing to detect all the samples of Neuroquila.A, and a few of the ACG.A samples accounted for the misses amongst the Polymorphic test-set, and a variety of misses were registered in the Standard set.

## Grisoft AVG v6.0 (28/6/99)

| | | | |
|---|---|---|---|
| ItW Overall | 99.1% | Macro | 98.3% |
| ItW Overall (o/a) | 99.1% | Standard | 98.6% |
| ItW File | 99.1% | Polymorphic | 96.8% |

*Grisoft's AVG* is yet another product to have benefitted from a recent makeover, and also features an on-access scanner for the first time in a *VB* review. The slightly unusual interface still forms the main operations centre, although improvements have been made to ease the task of configuration alteration.

Overall, this was a strong showing from *AVG* – detection rates were respectably high across all the test-sets. Previous problems that have been encountered with detection of infected floppy boot sectors with invalid BPB's appear to have been fixed, and all the ItW boot viruses were detected, both on-demand and on-access. Unfortunately however, Win95/Padania was missed in the ItW file set, keeping the VB 100% award at bay.

In terms of speed, *AVG* is at the lower end of the products tested for scanning executables, although far speedier when it comes to OLE2 files. Unfortunately however, the in-built heuristics which are responsible for a good proportion of the correct detections in the above tests, led to unwelcome false positives in the speed tests.

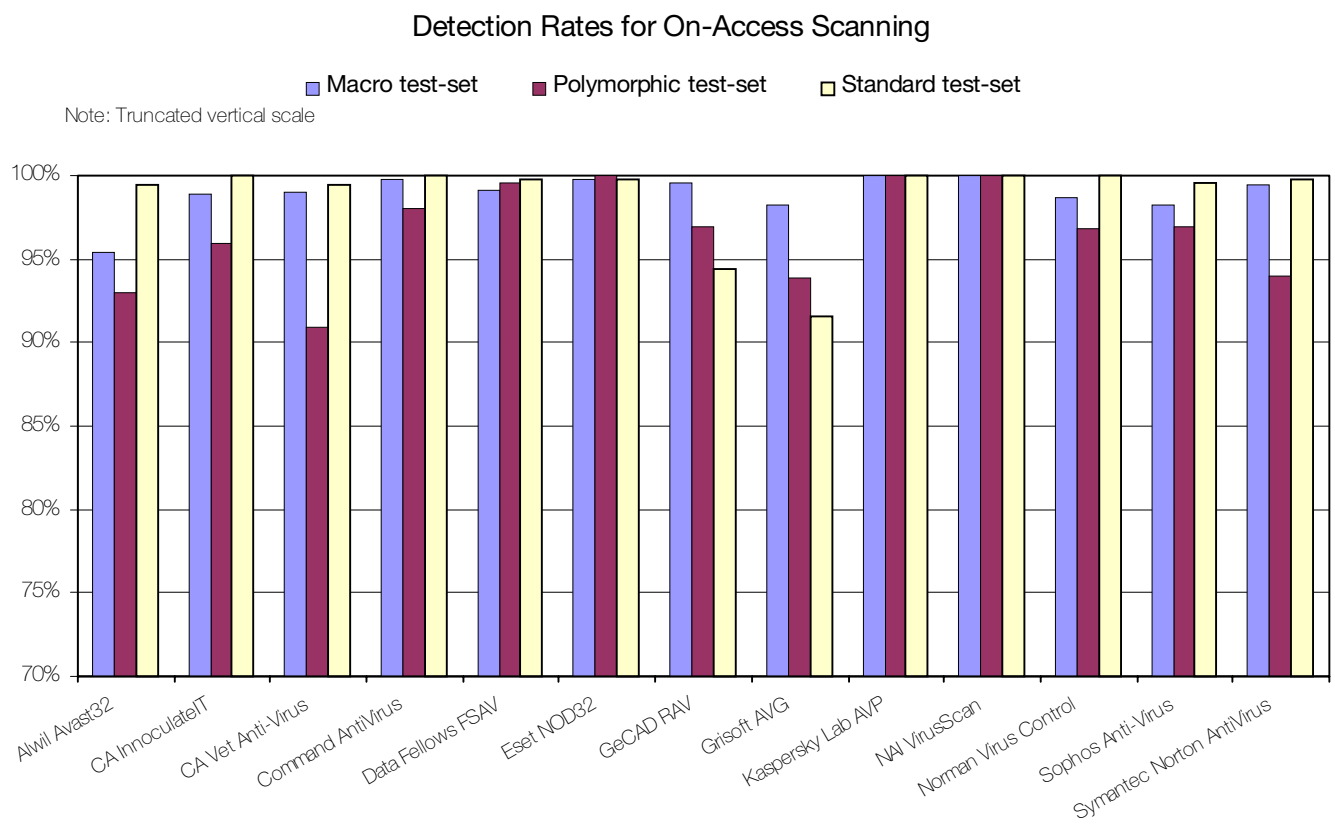
## Kaspersky Lab AVP v3.0.131 (30/6/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 100.0% |
| ItW Overall (o/a) | 100.0% | Standard | 100.0% |
| ItW File | 100.0% | Polymorphic | 100.0% |

Long the recipient of praise for achieving high detection rates, *Kaspersky Lab's AVP* detected all of the samples during on-demand scanning this time around, and is thus the fifth claimant to the VB 100% award. After such an impressive start, the strength of this Russian product was driven home further when the achievement was repeated by the on-access scanner. Impressive indeed.

The only blemish on the product occurred during the speed tests where two executable files were falsely identified as suspicious, and a third was declared to be corrupted. As noted for *AVG*, this is the negative effect of the heuristics which help to boost the detection rates. *AVP* is in the upper half of the field in terms of scanning speed.

The on-access scanner, giving an overhead of just over 200%, imposes itself a little more than some of the other scanners, but was far from the worst in this respect.




## NAI VirusScan NT v4.03a.4032 (30/6/99)

| | | | |
|---|---|---|---|
| ItW Overall | 99.9% | Macro | 99.9% |
| ItW Overall (o/a) | 99.9% | Standard | 100.0% |
| ItW File | 99.9% | Polymorphic | 100.0% |

Though not a clean sweep as for its alphabetical predecessor, *Network Associate's VirusScan NT* is following hot in *AVP's* footsteps.

This is due partly to the fact that the default file extension list has finally been updated such that file types associated with viruses known to be in-the-wild are scanned by default. Only the extensionless samples of the A, B, C and D variants of O97M/Tristate were missed throughout the test-sets in both on-demand and on-access scanning.

*VirusScan* is in the middle of the pack when it comes to scanning speed and on-access scanner overhead. Pleasingly, no false positives were detected during the speed tests.

## Norman Virus Control v4.70 (1/7/99)

| | | | |
|---|---|---|---|
| ItW Overall | 100.0% | Macro | 99.8% |
| ItW Overall (o/a) | 99.0% | Standard | 100.0% |
| ItW File | 100.0% | Polymorphic | 96.9% |

Recently featured in a standalone review (see *VB*, August 1999, p.21) *Norman Virus Control* (*NVC*) is the final product of this comparative to detect all the ItW File and Boot viruses during on-demand scanning, and thus achieve the VB 100% award.

On-demand scanning was reasonably quick, and three viruses account for all the misses that were observed – ACG.A, W97M/Stat.A and a document template infected with WM/Triple.B. Results were not so promising during on-access scanning however, exposing a slight weakness in *NVC*. Three ItW boot virus samples were missed (those with invalid BPB's), as were samples infected with XM/Compat.A and O97M/Tristate.C in the ItW file set.

## Proland Protector Plus v6.6

| | | | |
|---|---|---|---|
| ItW Overall | 89.4% | Macro | 62.8% |
| ItW Overall (o/a) | n/a | Standard | 65.2% |
| ItW File | 89.2% | Polymorphic | 22.1% |

In the last *VB* review of *Proland's NT* offering, it was mentioned that the product had some 'maturing' to do. Well, six months have passed by since then, and a greater degree of maturity is certainly evident in the results presented this time around.

An awful lot of samples were still missed from the Macro, Standard and Polymorphic test-sets however, especially the latter. The results clearly indicate that *Proland's* developers have focused predominantly upon ItW virus detection.

Whilst performing the speed tests, it was not possible to complete a scan of the OLE2 file set, due to a recurring application error. Consequently scanning speed results are limited to the scanning of executables. The decrease in scanning speed compared to that observed previously is concurrent with the general increase in the detection rates.

## Sophos Anti-Virus v3.23

| | | | |
|---|---|---|---|
| ItW Overall | 98.1% | Macro | 98.2% |
| ItW Overall (o/a) | 98.1% | Standard | 99.5% |
| ItW File | 97.9% | Polymorphic | 96.9% |

Failure to detect samples infected with Win95/Padania and O97M/Tristate.C prevented *Sophos Anti-Virus* (*SAV*) from achieving complete detection of the ItW viruses.

From the log files produced during on-demand scanning, a slight oddity with the treatment of the extensionless 'Book1' samples infected with O97M/Tristate was noticed. Notably, some were scanned and successfully detected, despite the scanner configuration supposedly excluding files with no extension. It transpired that a minor bug in the product (no longer present in the current product) caused such files to be scanned – a 'positive' bug in this case!

In terms of stability *SAV* proved to be one of the top products again, reliably detecting all the boot sector viruses in both on-demand and on-access scanning. It was also one of the few products whose on-access scanner was up to the standard of the on-demand scanner. This will, no doubt, stand it in good stead when on-access scanning is introduced into the VB 100% awards, as of the next comparative in the November issue.

## Stiller Integrity Master v4.21a

| | | | |
|---|---|---|---|
| ItW Overall | 66.7% | Macro | 50.2% |
| ItW Overall (o/a) | n/a | Standard | 83.9% |
| ItW File | 64.5% | Polymorphic | 29.8% |

The detection rate percentages quoted here for *Stiller Integrity Master* (*IM*), are included only for continuity's sake really. The product is not an anti-virus scanner – it is primarily an integrity checker. As such it does perform a scan of a system prior to building its checksum database. Since the virus scanner is only a minor part of the *IM* product, updates are not frequently available, and thus detection rates are not high.

To compare the results directly to those obtained for the other products would be equivalent to comparing apples to oranges. The results may be of interest to some of our readers who may use *IM* however, hence their inclusion.

Unsurprisingly, the relatively static arena of boot viruses is where *IM* performs best, detecting all the ItW boot viruses. Elsewhere in the test-sets where changes over the past year have been fast and furious, the percentages are lower, especially in the Macro and Polymorphic test-sets.

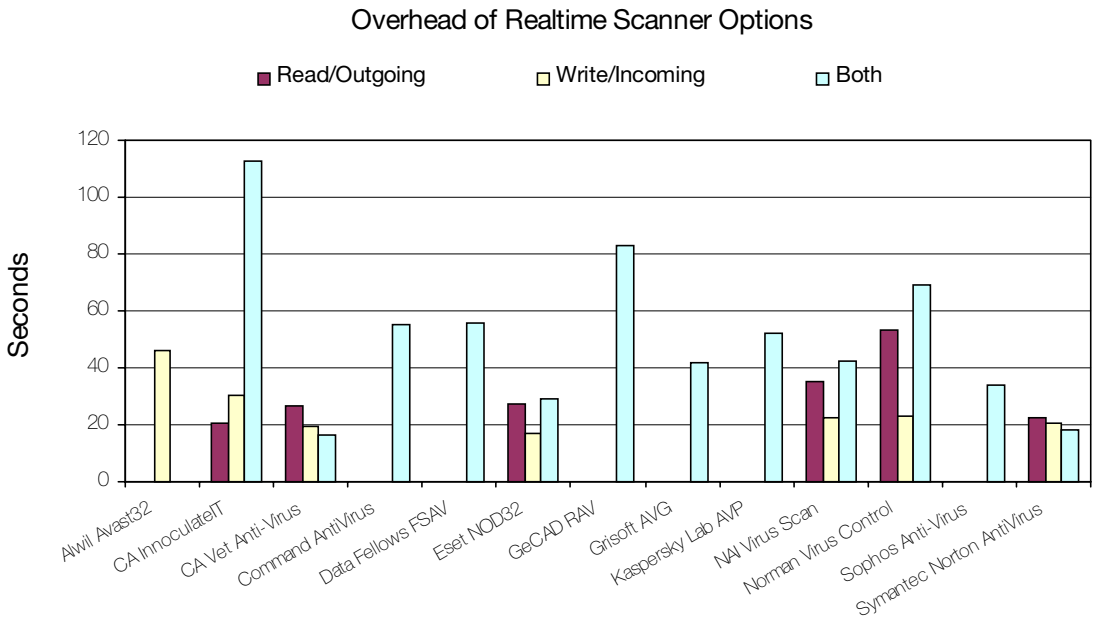
## Symantec Norton AntiVirus v5.02.01

| | | | |
|---|---|---|---|
| ItW Overall | 99.8% | Macro | 99.4% |
| ItW Overall (o/a) | 99.8% | Standard | 99.7% |
| ItW File | 100.0% | Polymorphic | 93.9% |

Failure to implement complete detection of Win95/Fono infected boot sectors (as noted in previous reviews) in both on-demand and on-access scanning, once again prevents *Symantec's NAV* from claiming the VB 100% award.

Elsewhere, detection rates were admirable, and misses were few and far between. Samples infected with PP97M/Vic.A, W97M/Lys (B, C and D variants) were missed in the Macro set, and the only miss in the Standard set was an executable sample infected with {W95/W97M}/Heathen.A. The lowest detection rate was observed in the Polymorphic set, due to the product's failure to detect samples infected with the A and B variants of ACG.

Identical results were obtained for on-access scanning – a fact that few products can boast about. The overhead of the on-access scanner was the lowest out of all the products tested, whereas the on-demand scanning speed of *NAV* was fairly average, and in keeping with the bulk of the products. The *Bloodhound* heuristics employed by default in *NAV* did not register any false positives during scanning of the clean executable and OLE2 file sets.



| | Hard Disk Scanning Speed | | | | | |
|---|---|---|---|---|---|---|
| | Executables | | | OLE2 files | | |
| | Time (min:sec) | Throughput (kB/s) | FPs [susp] | Time (min:sec) | Throughput (kB/s) | FPs [susp] |
| **Alwil Avast32** | 21:43 | 419.7 | 1 | 2:18 | 496.4 | 0 |
| **CA InnoculateIT** | 6:44 | 1353.8 | 0 | 0:28 | 2446.5 | 0 |
| **CA Vet Anti-Virus** | 10:20 | 882.1 | [1] | 0:17 | 4029.5 | 0 |
| **Command AntiVirus** | 6:27 | 1413.3 | 0 | 0:29 | 2362.1 | 0 |
| **Data Fellows FSAV** | 14:10 | 643.4 | [3] | 0:48 | 1427.1 | 0 |
| **Dialogue Science DrWeb32** | 17:42 | 515.0 | 1+[18] | 0:52 | 1317.3 | [1] |
| **Eset NOD32** | 3:12 | 2848.6 | 0 | 0:23 | 2978.3 | 0 |
| **GeCAD RAV** | 23:04 | 395.2 | [1] | 1:02 | 1104.9 | 0 |
| **Grisoft AVG** | 14:29 | 629.4 | 10 | 0:23 | 2978.3 | 0 |
| **Kaspersky Lab AVP** | 3:50 | 2378.0 | [2] | 0:39 | 1756.4 | 0 |
| **NAI VirusScan** | 10:40 | 854.6 | 0 | 0:48 | 1427.1 | 0 |
| **Norman Virus Control** | 6:30 | 1402.4 | 0 | 0:34 | 2014.8 | 0 |
| **Proland Protector Plus** | 4:51 | 1879.5 | 5 | n/t | n/t | n/t |
| **Sophos Anti-Virus** | 11:20 | 804.3 | 0 | 0:33 | 2075.8 | 0 |
| **Stiller Integrity Master** | 5:33 | 1642.4 | 1+[47] | 0:53 | 1292.5 | 1 |
| **Symantec Norton AntiVirus** | 8:41 | 1049.8 | 0 | 0:42 | 1631.0 | 0 |

### For the 100th time...

Recent events have led us to believe that it is time we reminded ourselves exactly what the VB 100% award is all about. Just who is it designed to benefit? Does it provide the definitive standard to which products should aspire? The sole criterion of a 'good' product?

By simple definition, the VB 100% award is a certification scheme which identifies products capable of detecting all the viruses currently in-the-wild (as defined by the WildList Organisation) *at the time of testing*. The time dependancy of the award is fundamental to its usefulness. Unlike for some of the other certification schemes out there, recent WildLists are used for the VB 100% award. In this comparative, for example, products had to be submitted by 2 July, and the ItW testing was performed against a June WildList (which was announced in mid-June). The award logos which are issued to the appropriate vendors can quite justifiably be reproduced by the anti-virus developers as a marketing aid. By doing so, users familiar with the scheme can quickly spot products of good pedigree.

This last comment is important – of good pedigree. Not 'the best'. *Virus Bulletin* receives no end of enquiries as to the 'best' anti-virus product, from a variety of sources – both home users and corporates. The simplest yardstick by which to compare anti-virus products is detection rate. The VB 100% award gives an at-a-glance picture of products that did, and those that did not, 'make the grade' during the tests. Thus, following the results across a series of tests enables the leading products to be easily identified.

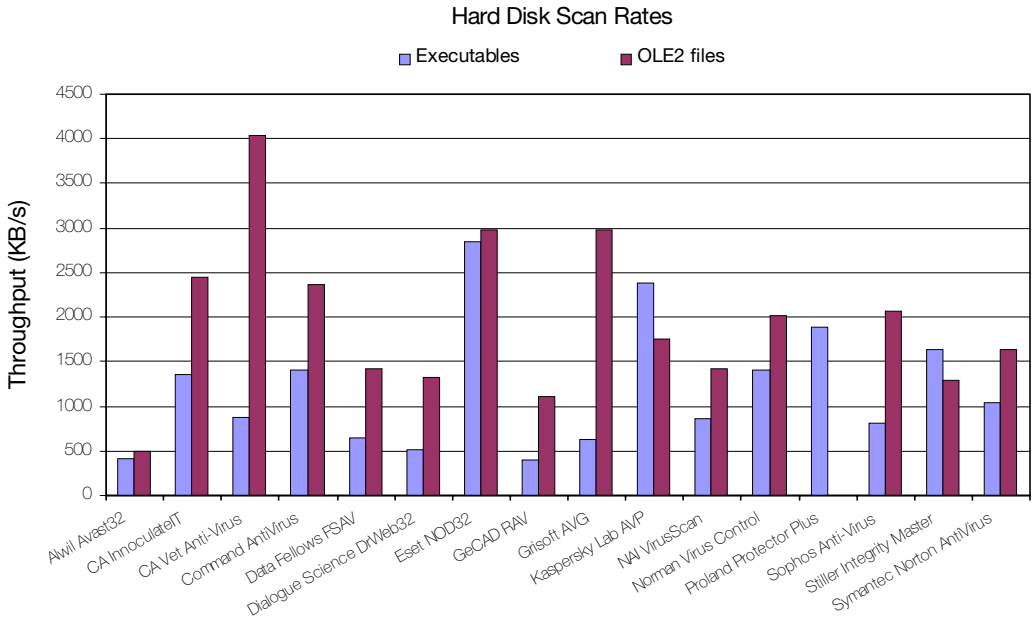
Whether looking from within the anti-virus circle or not, it is obvious that an awful lot of factors besides detection rates are important in selecting the most suitable product. A more accurate description of equipping oneself with virus protection might be to speak of it in terms of an anti-virus *service* – a package that in addition to the product itself, includes ongoing updates, technical support, and the like. The VB 100% award includes no measure of such factors, and as such is not itself a measure of the 'best' product.

The developers of each product obviously want to receive the VB 100% award for each test entered. The desire to do so has no doubt resulted in the improvement of many of the on-demand scanners. However, as with any certification process there is a danger in its over-emphasis. As mentioned above, it is a measure of only one aspect of a product's capabilities.

The anti-virus industry itself is partly responsible for the over-emphasis on certification schemes. The anti-virus marketing arena is an aggressive area, in which vendors do not pull any punches. Decorating products with the accolades of certifications A through Z is no doubt a successful

marketing tool. And why should this not be the case? Where earned, it is perfectly fair for products to bear the fruits of their labour.

Recently however, *Virus Bulletin* has noticed a couple of the anti-virus vendors displaying an altered VB 100% logo, one with the date removed. A marketroid's dream – an ageless certification scheme, once passed, forever qualified.




Besides being a breach of the conditions under which the award is handed out, more importantly, such an act fully intends to mislead the very people the VB 100% award is designed to help – users seeking genuine, impartial anti-virus advice.

In summary, the VB 100% awards are not by themselves an adequate summation of the entire results observed during a comparative review. Instead they provide the readers with a quick guide to the products which have been best kept up to date with changes in the virus scene, and they provide the vendors with a widely recognized mark of achievement.

### Changes to the VB 100% Award

Since its introduction in January 1998, the VB 100% certification scheme has concentrated solely upon on-demand scanning. However, much anti-virus protection nowadays is centered upon on-access scanning. As such, the VB 100% certification scheme is evolving to incorporate on-access scanning as from the next comparative in the November 1999 issue.

Thus far, the VB 100% award has certainly been a success in that whilst striving to pass the regular certification tests, the anti-virus products have no doubt improved. With the inclusion of on-access scanning into the certification scheme as from the next comparative review, we hope this improvement will carry forth into the world of the on-access scanners, undoubtedly the weakest feature of the products in general.

### Summary

Returning to the results presented in this review, it is clear that for most of the products tested, high detection rates across the board were observed. *Kaspersky Lab's AVP* steals the limelight with its detection of all the samples in both on-demand and on-access scanning. Close on its heels are *NOD32* from *Eset*, which detected all the ItW samples in on-demand and on-access tests, and *NAI's VirusScan* which but for its failure to detect extensionless samples, would also have achieved a clean sweep. Needless to say, both *AVP* and *NOD32* earn the VB 100% award this month. Four other products also managed to detect all the ItW viruses during on-demand scanning – *Norman Virus Control*, *GeCAD's RAV* and *Computer Associate's* brace of anti-virus products, *Vet Anti-Virus* and *InnoculateIT*. Interestingly, out of these six VB 100% clad products only *AVP* and *NOD32* manage to achieve the same standard during on-access scanning.

It is pleasing to note that *PowerPoint* file formats now seem to be supported by all the major products, at least in on-demand scanning. The same is not true of *Access* files, and so four of the sixteen products missed samples infected with A97M/Accessiv variants. Also surprising was the observation that password protected files, are still ignored by certain products. Thus *Word* document samples infected with W97M/Pwd.A were missed.

**Technical Details**

**Test Environment:** Server: *Compaq Prolinea 590*, 90MHz Pentium with 80 MB of RAM, 2 GB hard disk, running *NetWare 4.10*. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB RAM, 4 GB hard disks, CD-ROM and 3.5-inch floppy, all running *Windows NT* with *Service Pack 5* applied. The workstations could be rebuilt from image back-ups, and the test-sets were stored in a read-only directory on the server. All timed tests were performed on a single machine that was not connected to the network for the duration of the timed tests, but was otherwise configured identically to that described above.

**Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NT/199909/test_sets.html.

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