COMPARATIVE REVIEW

WOW! Wide Open Windows

Six months on from the last *Windows 98* Comparative, the time has come again to take a look at the products for the pre-*Windows 2000* operating system.

Sixteen products were submitted for review, the only notable absentees being *Trend Micro* (who have not submitted since March), and *Panda Software* (who intend to start submitting at the start of next year).

Test-sets and Procedures

Three essentially identical machines were used for testing, the details of which can be found at the end of this review. As usual for *VB* Comparatives, the timed tests were all performed on a single machine, isolated from the network. The only change made to the familiar *VB* tests was the introduction of *PowerPoint* files into the clean OLE2 set and the file set used in the overhead tests.

All products were presented with the customary *VB* test-sets – that is, the Polymorphic, Standard, Macro and In the Wild (ItW) sets. The ItW set, with its boot and file virus components, was aligned to the August 1999 WildList, which was announced a couple of weeks prior to the product submission deadline (31 August).

The overall WildList is reduced somewhat from that used in the previous Comparative. Concurrent with the decrease in the prevalence of boot sector viruses, only 33 made up the boot sector test, compared to the 84 that were present this time last year. Other departures include the file viruses Green Caterpillar, Quicky.1376, Raadioga, Spanska.1500 and Tai-Pan.666. On the macro virus front, farewells are due to WM/NiceDay.A, WM/Wazzu.F and XM/Laroux.FC to name but a few. The only new appearances in the ItW set were macro viruses, and included W97M/Chack.H, W97M/Melissa.I, X97M/Laroux.CF and W97M/Ethan.B.

No changes to the Polymorphic test-set were made this time, but the Standard and Macro test-sets were updated with a selection of viruses. Of particular interest is the addition of Visual Basic Script (VBS) viruses for the first time in *VB* tests. On this front, VBS/Freelinks, VBS/Happy and three variants of VBS/First were included. A few sightings of VBS/Freelinks (see p.6 for analysis) in the wild were noted at the start of July.

The standard method of assessing the overhead of each of the on-access scanners was used once more. The time taken to copy a set of 200 files between directories on a local hard disk was measured with the scanners in each of its various configurations. The file set consisted of 200 files totalling 25.9MB, containing a mixture of executables, *Word*, *Excel* and *PowerPoint* documents. The scanning speed of each of the on-demand scanners was measured for scanning both executables and OLE2 (*Word*, *Excel* and *PowerPoint*) files. These timed scans also serve as false positive tests, since both of the file sets are clean.

The detection rate percentages printed in each of the product summaries are those for on-demand scanning, unless otherwise indicated – 'o/a' being on-access.

Aladdin eSafe Protect v2.1 (1/9/99)

ITW Overall	98.0%	Macro	96.1%
ITW Overall (o/a)	98.0%	Standard	97.4%
ITW File	97.9%	Polymorphic	92.9%

Aladdin Knowledge Systems' eSafe Protect is a product packed with a whole host of features – anti-virus protection being just one. Inserting the CD produces the standard installation front screen, where aside from proceeding with the installation, options to view the user manual, a demo and a white paper are presented. Unfortunately, for those using a screen resolution less than 800x600 pixels, scrolling of this screen is not possible, preventing access to any of the options!

Though not achieving the highest detection rates, particularly in the Macro and Polymorphic sets, no problems were encountered during the testing of *eSafe Protect* – something that cannot be boasted by a few of the other products in this review. Pleasingly, the on-access scanner of *eSafe Protect* proved perfectly stable throughout both the detection and overhead tests. The only slight niggle is the lack of a 'keypress option' during scanning of floppy boot sectors.

The detection rates in the Macro and Polymorphic test-sets are perhaps the weakest areas of this product. *eSafe Protect's* detection of infected document templates has been noted as a weakness in previous reviews, and it still seems to be an area of concern now. Eight DOT files (infected with Carr.A, Class.F, Groov.D, Metamorph.A, Nottice.A and Walker.B), remained undetected, despite the corresponding DOC files being successfully detected.

Alwil Avast32 v3 (26/8/99)

ITW Overall	100.0%	Macro	95.2%
ITW Overall (o/a)	99.8%	Standard	96.9%
ITW File	100.0%	Polymorphic	99.9%

As with all previous *VB* Comparatives, the on-demand scanning rates in this review have been determined from the products' scanning logs. Unfortunately for *Avast32*,

On-demand tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Missed	%	Missed	%	%	Missed	%	Missed	%	Missed	%
Aladdin eSafe Protect	0	100.0%	11	97.9%	98.0%	143	96.1%	425	92.9%	31	97.4%
Alwil Avast32	0	100.0%	0	100.0%	100.0%	162	95.2%	9	99.9%	34	96.9%
CA InoculateIT	0	100.0%	0	100.0%	100.0%	0	100.0%	5	99.9%	0	100.0%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	28	99.2%	264	93.9%	1	99.9%
Command AntiVirus	0	100.0%	0	100.0%	100.0%	14	99.6%	112	98.0%	3	99.7%
Data Fellows FSAV	0	100.0%	1	99.9%	99.9%	3	99.9%	0	100.0%	8	98.9%
Dialogue Science DrWeb32	0	100.0%	0	100.0%	100.0%	17	99.4%	0	100.0%	4	99.5%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	3	99.7%
FRISK F-Prot	0	100.0%	0	100.0%	100.0%	25	99.6%	18	99.6%	3	99.7%
GeCAD RAV	0	100.0%	0	100.0%	100.0%	0	100.0%	3	99.9%	4	99.5%
Grisoft AVG	0	100.0%	8	98.1%	98.2%	87	97.3%	96	96.8%	43	97.3%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	4	99.6%
NAI VirusScan	0	100.0%	1	99.9%	99.9%	7	99.8%	0	100.0%	12	98.4%
Norman Virus Control	0	100.0%	0	100.0%	100.0%	12	99.6%	174	96.9%	1	99.8%
Sophos Anti-Virus	0	100.0%	0	100.0%	100.0%	15	99.4%	174	96.9%	20	98.4%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	18	99.3%	264	93.9%	1	99.7%

when set to scan the entire test-set, the latter half of the scanning log was observed to have been corrupted. To circumvent this problem, the test-set had to be scanned in chunks, producing smaller, but uncorrupted log files.

At first sight the detection rates against the ItW set look impressive – the only hurdle between *Avast32* and the VB 100% award being samples of CIH.1003 and CIH.101x, that were missed by the on-access scanner. Similar discrepancies between the on-demand and on-access scanner detection rates were also seen elsewhere in the test-sets.

Scanning of the infected floppy boot sectors proved fairly laborious, thanks partly to the lack of a multiple diskette prompt. However, all the boot viruses were detected, for both on-demand and on-access scanning.

Testing of the on-access scanner proved problematic. Due to the lack of a 'deny access' option, the scanner was set to scan on file writes and delete infected files, whilst the test-set was copied to a local hard drive. The copied files were then copied to a new location on the local hard drive, and this process repeated until no further detections were noted. Unfortunately, the sheer number of files in the test-set caused problems for the scanner, and so it had to be copied across in more 'bite-size' chunks. Even so, the number of files in the Polymorphic set still caused problems for the scanner, and so no results are presented here for this set.

Speed-wise, *Avast32* is at the slower end of the pack, particularly when it comes to scanning OLE2 files, but the overhead of the on-access scanner is in keeping with the bulk of products. One false positive was reported in the Clean set – an EXE file infected with Tequila.2468.

CA InoculateIT v4.53 (28/6/99)

ITW Overall	100.0%	Macro	100.0%
ITW Overall (o/a)	98.8%	Standard	100.0%
ITW File	100.0%	Polymorphic	99.9%

Computer Associates' InoculateIT has picked up the VB 100% award in the last three rounds of comparative product testing. A quick glance at the the percentages obtained here for on-demand scanning reveal another impressive performance in terms of detection. Out of the file viruses, only five samples of ACG.A were missed across all the test-sets. The on-demand scanner defaults to scan all files, but curiously the on-access component scans by file extension only. The default list was sadly a few months behind schedule, and so a multitude of *PowerPoint*, *Access* and infected screen-saver (SCR) files slipped through the net during the on-access tests. Additionally, failure of the on-access scanner to detect a Michelangelo-infected floppy disk pushed the VB 100% award further from the grasp of *InoculateIT* this time around.

On-access tests	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Missed	%	Missed	%	%	Missed	%	Missed	%	Missed	%
Aladdin eSafe Protect	0	100.0%	11	97.9%	98.0%	143	96.1%	425	92.9%	31	97.4%
Alwil Avast32	0	100.0%	2	99.7%	99.8%	154	95.5%	n/t	n/t	16	98.8%
CA InoculateIT	1	96.9%	16	99.0%	98.8%	33	99.0%	251	98.9%	8	98.9%
CA Vet Anti-Virus	0	100.0%	0	100.0%	100.0%	28	99.2%	264	93.9%	1	99.9%
Command AntiVirus	0	100.0%	0	100.0%	100.0%	14	99.6%	112	98.0%	3	99.7%
Data Fellows FSAV	0	100.0%	1	99.9%	99.9%	3	99.9%	0	100.0%	8	98.9%
Dialogue Science DrWeb32	0	100.0%	0	100.0%	100.0%	17	99.4%	0	100.0%	4	99.5%
Eset NOD32	0	100.0%	0	100.0%	100.0%	4	99.8%	0	100.0%	3	99.7%
FRISK F-Prot	1	96.9%	1	99.9%	99.7%	78	98.7%	n/t	n/t	3	99.7%
GeCAD RAV	0	100.0%	0	100.0%	100.0%	45	98.5%	33	99.0%	25	98.1%
Grisoft AVG	1	96.9%	9	98.0%	98.0%	93	97.2%	268	93.9%	116	91.5%
Kaspersky Lab AVP	0	100.0%	0	100.0%	100.0%	5	99.8%	0	100.0%	3	99.7%
NAI VirusScan	0	100.0%	1	99.9%	99.9%	7	99.8%	0	100.0%	14	98.2%
Norman Virus Control	0	100.0%	0	100.0%	100.0%	12	99.6%	174	96.9%	1	99.8%
Sophos Anti-Virus	0	100.0%	3	99.7%	99.7%	32	98.9%	174	96.9%	20	98.4%
Symantec Norton AntiVirus	0	100.0%	0	100.0%	100.0%	18	99.3%	264	93.9%	1	99.7%

A couple of minor problems which have been mentioned in previous reviews unfortunately still remain, including false warnings about viruses in memory following a reboot. Also, the product managed to detect a previous installation of itself despite the fact that is was being installed onto a freshly imaged machine.

CA Vet Anti-Virus v10.1.0 (31/8/99)

ITW Overall	100.0%	Macro	99.2%
ITW Overall (o/a)	100.0%	Standard	99.9%
ITW File	100.0%	Polymorphic	93.9%

Despite the ownership change, *Vet Anti-Virus* still remains a pleasant and easy product to test. Identical detection rates were observed for both on-demand and on-access scanning, and detection of the ItW file and boot sets was complete, earning *Vet* its second VB 100% award this year.

One sample of Win32/Parvo in the Standard set, and a handful of X97M/Laroux variants in the Macro set account for the bulk of the misses. Additionally, there seem to be problems in detecting samples infected with the polymorphic X97M/Soldier.A and XM/Soldier.A. Failure to detect samples infected with the A and B variants of ACG account for the misses in the Polymorphic set.

Historically one of the fastest scanners, recent results suggest that it no longer occupies the prime perch in this sense – scanning rates seem to be slightly slower than those previously observed.

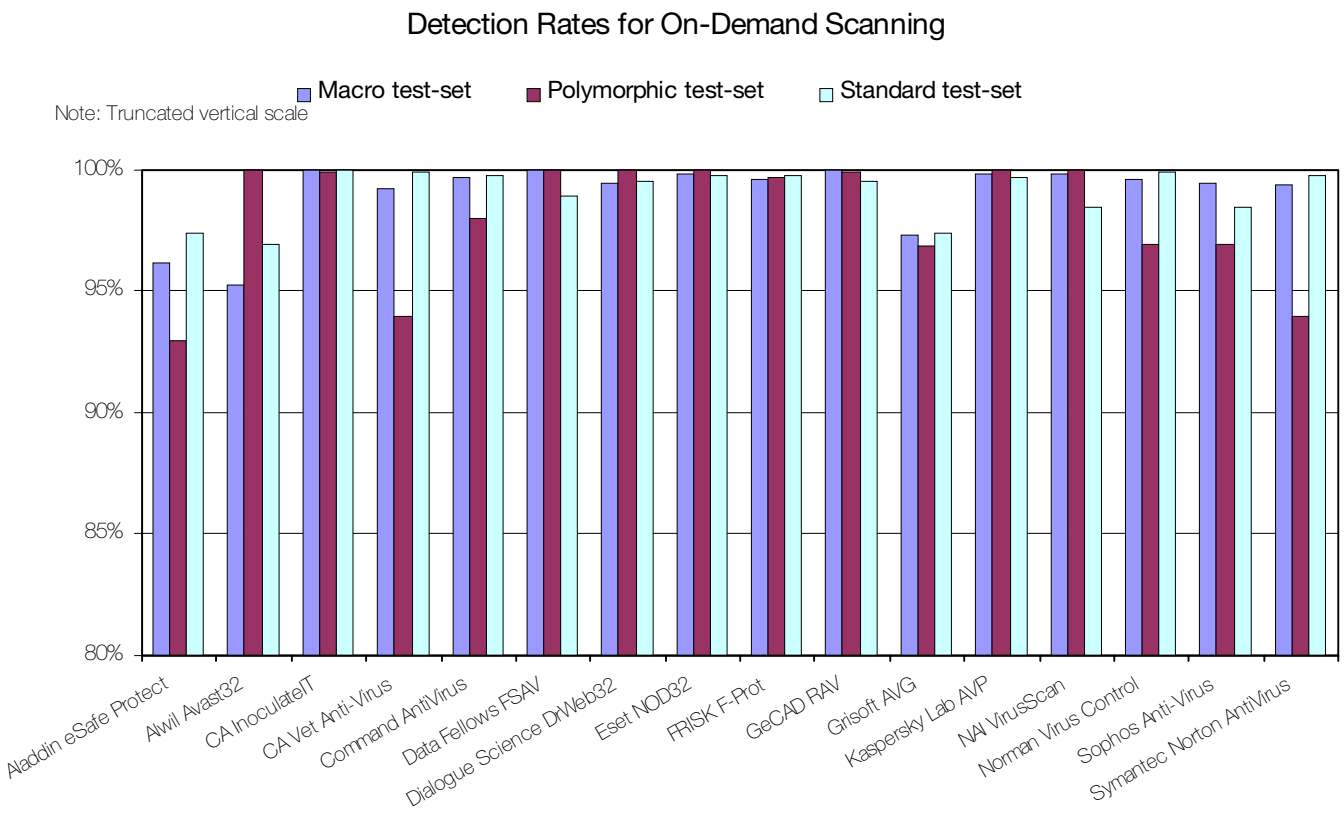
Command AntiVirus v4.57 (30/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	98.0%

The second recipient of the VB 100% award this month is *Command Software AntiVirus* (*CSAV*). Impressive detection rates were observed across all the test-sets.

Both the on-demand and on-access scanners are configured by default to scan files of certain extensions only. However, unlike other similarly configured products, the extension lists have clearly been kept up to date. Interestingly, two of the three VBS/Freelinks samples were missed, as was the JavaScript (JS) file infected with VBS/First.C.

One gripe with *CSAV's* on-access scanner is that it did not appear possible to turn off the on-screen messaging, which caused the test machine to become unstable when scanning the entire test-set.



Data Fellows FSAV v4.05 (25/8/99)

ITW Overall	99.9%	Macro	99.9%
ITW Overall (o/a)	99.9%	Standard	98.9%
ITW File	99.9%	Polymorphic	100.0%

Thanks to its use of two virus engines (*F-Prot* and *AVP*), the double-barrelled anti-virus protection provided by *Data Fellows F-Secure Anti-Virus* (*FSAV*) gives the expected high detection rates across all the test sets. As ever, the downside of the increased armoury is the scanning speed, which was observed to be at the slower end of the range observed across all the products.

Since its last appearance in a *VB* Comparative, detection of infected *PowerPoint* files is now firmly in place in *FSAV*. In fact, only a handful of samples were missed across all the test-sets, for both on-demand and on-access scanning. Unfortunately, the failure to scan extensionless samples prevented *FSAV* achieving the VB 100% award, since the BOOK1 samples infected with the A, B, C and D variants of Tristate were missed.

VBS/Freelinks, VBS/Happy and VBS/First samples were missed during both on-demand and on-access scanning. The samples were detected when the necessary file extensions were included in the default 'to scan' list, or the product reconfigured to scan all files.

Three clean files were flagged as suspicious (by one or both of the engines) during scanning of the Clean set. The overhead of *GateKeeper*, the on-access scanner, was just below the average of that observed from all the products.

Dialogue Science DrWeb32 v4.12a (30/8/99)

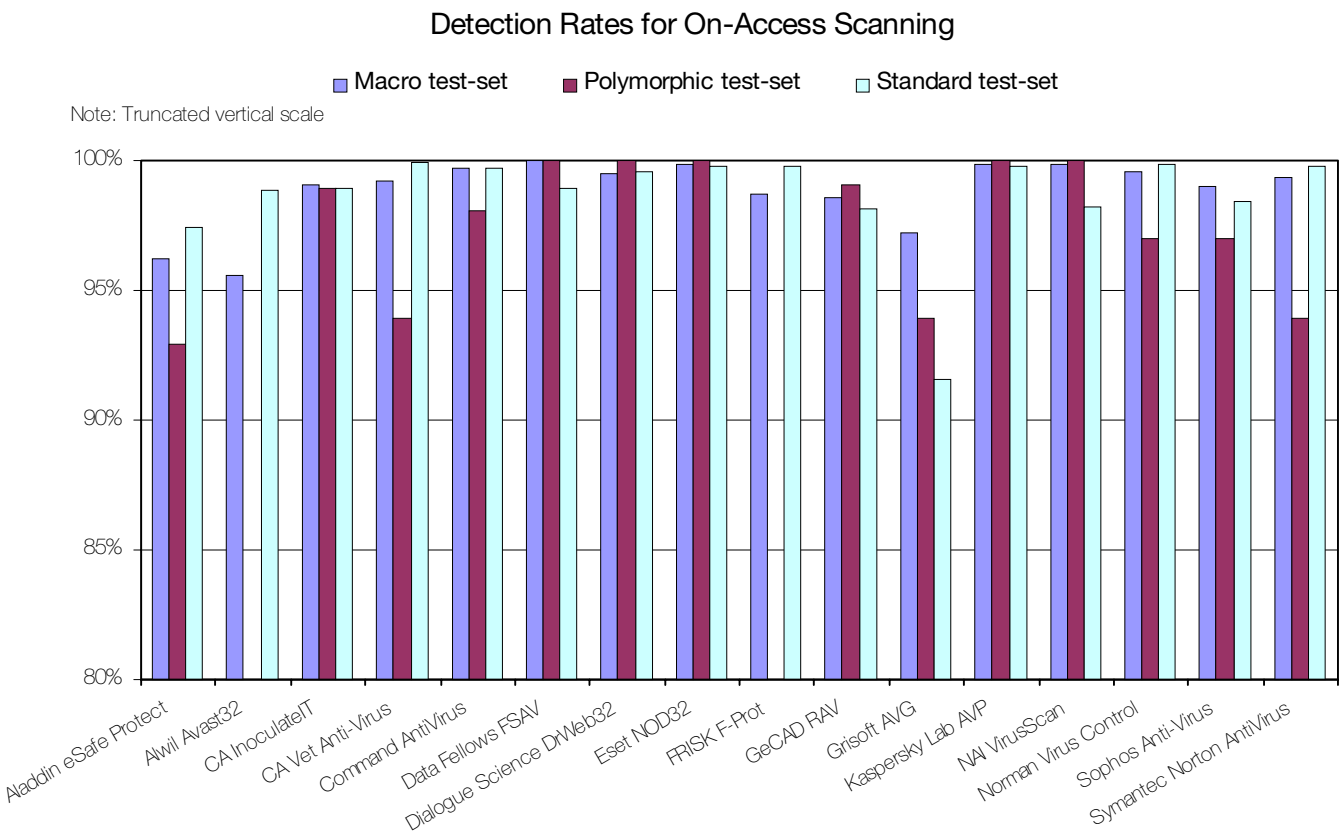
ITW Overall	100.0%	Macro	99.4%
ITW Overall (o/a)	100.0%	Standard	99.5%
ITW File	100.0%	Polymorphic	100.0%

Impressively high detection rates across the board ensure that *DrWeb32* maintains its VB 100% record on the *Win 98* platform, and picks up its second VB 100% award this year.

The high detection rates are due partly at least to the use of heuristics. Traditionally, this can have the downside of causing false positives to be registered, a fact that was in evidence during the speed tests, where one and 17 files were flagged as infected and suspicious, respectively.

SpIDer Guard, the on-access component, is a relatively new addition to the *DrWeb32* product, and made its first appearance in *VB* tests in May 1999. Detection-wise, its performance is excellent, the detection rates mirroring those of the on-demand scanner. Unfortunately however, it is let down by its stability. Problems were encountered during the on-access boot sector tests. Attempting to access diskettes infected with either Boot-437 or Cruel caused the machine to hang, irrespective of the configuration settings of *SpIDer Guard*. However, since both viruses were detected and identified successfully, the 100% scoreline remains.

SpIDer Guard is definitely the weakest component of the *Dialogue Science* anti-virus package. Aside from its slight stability problems, the overhead of *SpIDer Guard* was amongst the largest observed for all the products.



Eset NOD32 v1.24 (30/8/99)

ITW Overall	100.0%	Macro	99.8%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	100.0%

The fourth recipient of a VB 100% award this month, *Eset's NOD32* puts in the usual strong performance that has come to become expected from this Slovak offering.

The high detection rates in the non-ItW sets owes some thanks at least to the use of heuristics in as well as to virus signatures. Only seven samples were missed over all the test-sets. *NOD32* also exhibited extremely impressive scanning speed, blitzing some of the other products with its scan rates well in excess of 2500kB/sec.

FRISK F-Prot for Windows v5.05c (30/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	99.7%	Standard	99.7%
ITW File	100.0%	Polymorphic	99.6%

In its first appearance in *VB* tests back in May, *F-Prot* for *Windows* (*FP-WIN*) returned impressive detection rates, and earned itself the VB 100% award. Unfortunately, this time around the award is lost due to the failure of the on-access scanner to detect the extensionless BOOK1 samples infected with O97M/Tristate.C, and the boot sector infected with Michelangelo.

When enabled, the 'deny access' option of the on-access scanner appeared to hang the test machine whenever access to an infected file was requested. Thus, the on-access detection rates have been determined from the scanning log created whilst attempting to copy the test-set to the local HD. Even this method proved problematic since *FP-WIN* consistently hung the test machine during copying of the Polymorphic set. As such, on-access detection rates against this set are not reported here.

The lower detection rates of the on-access scanner (*F-Stop*) are due mainly to the fact that heurisitics are not enabled by default, as they are for the on-demand scanner. Thus, the detection rates (particularly against the Macro set) are noticeably lower.

Further problems with the on-access scanner were encountered during the overhead tests. When configured to scan purely outgoing files, fatal exceptions were consistently observed. The same problem was not evident in any other configurations, even when set to scan both incoming and outgoing files. Four false positives and 12 suspicious files were registered during scanning of the Clean set. The scanning rates and on-access scanner overhead were in line with the average seen across the product range.

GeCAD RAV v7.0 (30/8/99)

ITW Overall	100.0%	Macro	100.0%
ITW Overall (o/a)	100.0%	Standard	99.5%
ITW File	100.0%	Polymorphic	99.9%

A regular participant in *VB* tests, and featured in a standalone review last month (see *VB*, October 1999, p.20), *Romanian Anti-Virus* (*RAV*) from *GeCAD Software* doubles its collection of VB 100% awards this month.

Unfortunately, as described for previous products, the test experience was not a particularly pleasant one – once again the problems centred around the on-access scanner, in this case, *RAV Monitor*. During initial tests (using a utility that attempts to open all of the files it comes across), access to almost half of the test-set samples was 'allowed'. The test was repeated by copying the test-set to the local HD with *RAV Monitor* configured to 'block' infected files. Fewer files were missed this time, although still far more than expected from the results of the on-demand scanning tests. Furthermore, the test-machine repeatedly hung during copying of an *Excel* file infected with O97M/Teocatl.A. The missed files were copied between locations on the local HD until no further detections were made – the final on-access results mirror those of the on-demand scanner.

Both the scanning speed and on-access scanner overhead were observed to be in line with those for the bulk of the products tested. Unfortunately, one file in the Clean set was flagged as suspicious.

Grisoft AVG 6.0.77 (31/8/99)

ITW Overall	98.2%	Macro	97.3%
ITW Overall (o/a)	98.0%	Standard	97.3%
ITW File	98.1%	Polymorphic	96.8%

Upon insertion of the *Grisoft AVG* CD, an HTML page is displayed from which the various installation options are presented. The updates submitted to this review were only compatible with the US product version, and so that was the version tested.

The *AVG* user interface is somewhat different to the bulk of anti-virus products, but once accustomed to it, the product is extremely simple to use.

Over recent Comparatives, the on-demand detection rates have been climbing, and once again a respectable performance is displayed. Unfortunately, *Word* files infected with W97M/Marker.O were missed in the ItW set, which coupled with the failure to detect Michelangelo infected boot sectors during on-access scanning, pulled the VB 100% from *AVG's* grasp.

Slightly poorer detection rates were observed during on-access scanning, but on the positive side it was noticed that no stability problems were experienced throughout testing.

The integrity checking facility, which is enabled by default, was disabled for the duration of the speed tests, where, unfortunately, seven false positives were registered, and two files flagged as suspicious.

Kaspersky Lab AVP v3.0.131 (28/8/99)

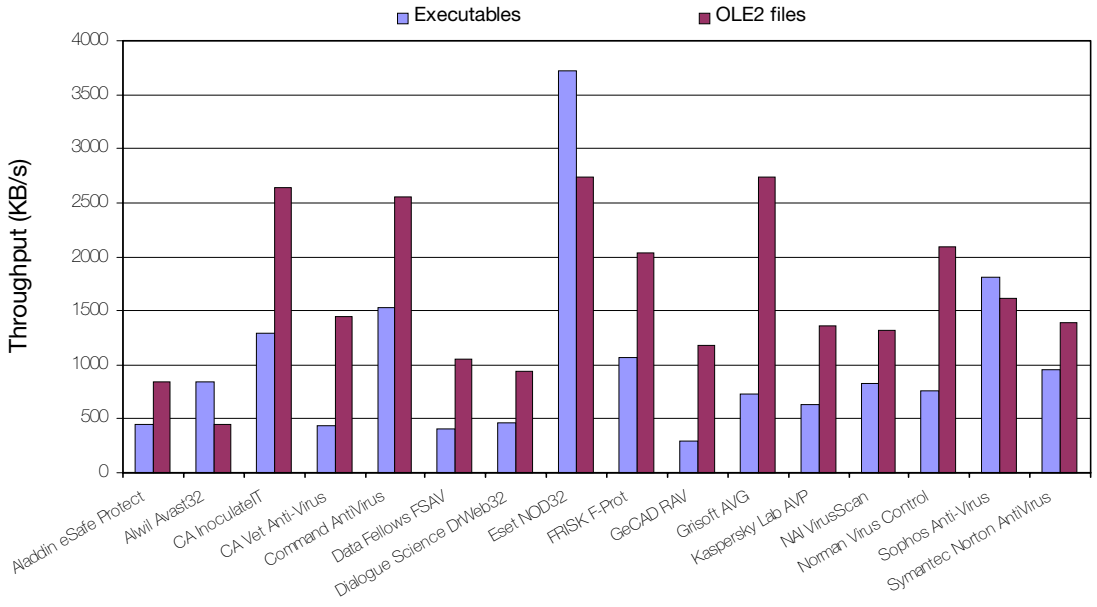
ITW Overall	100.0%	Macro	99.8%
ITW Overall (o/a)	100.0%	Standard	99.6%
ITW File	100.0%	Polymorphic	100.0%

Last time around it was a clean sweep for *Kaspersky Lab's AVP* – 100% detection of all the samples in the test-sets for on-demand scanning. The feat was not to be repeated this time, although results were sufficient for *AVP* to claim its tenth VB 100% award.

During both on-demand and on-access tests, all three of the VBS/Freelinks samples were missed, along with *Word* documents infected with W97M/Chack.AR. Also, the on-access scanner missed one of the XM/Laroux.F samples.

Problems were encountered during the speed and overhead tests, due to one of the executables in the Clean set – STAT.EXE. As soon as this file was copied between the HD locations during the overhead tests, with *AVP Monitor* enabled, the test machine slowed almost to a halt, some-

Hard Disk Scan Rates



	Hard Disk Scanning Speed					
	Executables			OLE2 files		
	Time (min:sec)	Throughput (kB/s)	FPs [susp]	Time (min:sec)	Throughput (kB/s)	FPs [susp]
Aladdin eSafe Protect	20:00	455.8	0	1:34	844.0	0
Alwil Avast32	10:52	838.9	1	2:59	443.2	0
CA InoculateIT	7:04	1289.9	0	0:30	2644.5	0
CA Vet Anti-Virus	21:05	432.4	0	0:55	1442.4	0
Command AntiVirus	5:59	1523.5	[12]	0:31	2559.2	0
Data Fellows FSAV	22:21	407.9	[3]	1:15	1057.8	0
Dialogue Science DrWeb32	19:35	465.5	1 + [17]	1:24	944.4	[1]
Eset NOD32	2:27	3720.6	0	0:29	2735.6	0
FRISK F-Prot	8:30	1072.4	4 + [12]	0:39	2034.2	0
GeCAD RAV	31:38	288.2	[1]	1:07	1184.1	0
Grisoft AVG	12:33	726.3	7 + [2]	0:29	2735.6	0
Kaspersky Lab AVP	14:29	629.4	0 +[2]	0:58	1367.8	0
NAI VirusScan	11:00	828.9	0	1:00	1322.2	0
Norman Virus Control	12:00	759.6	0	0:38	2087.7	0
Sophos Anti-Virus	5:00	1811.0	0	0:49	1619.1	0
Symantec Norton AntiVirus	9:36	949.5	0	0:57	1391.8	0

times hanging up completely. In order to measure meaningful overhead times, STAT.EXE was temporarily replaced by a similarly sized executable, and the tests repeated. The overhead of *AVP Monitor* was finally measured to be approximately 160% – in keeping with that for other products featured in this review.

NAI VirusScan v4.0.3.4040 (25/8/99)

ITW Overall	99.9%	Macro	99.8%
ITW Overall (o/a)	99.9%	Standard	98.4%
ITW File	99.9%	Polymorphic	100.0%

Returning very similar detection rates to those observed during testing of its *Windows NT* incarnation, *VirusScan* missed only a few samples across all the test-sets. Sadly, at least in terms of the VB 100% award, these included the extensionless BOOK1 samples infected with the four variants of O97M/Tristate.

On-access protection is provided with the *McAfee VShield*, which offers system scanning and email scanning (the latter was disabled throughout these tests). Other than two samples infected with Cruncher, the results of the on-demand and on-access scanners were identical.

VirusScan failed to detect samples infected with HLLP/Toadie variants – in this respect the product was certainly not alone. Samples of the relatively high profile (thanks to its potentially destructive payload) macro virus W97M/Thus were also missed.

Speed-wise, *VirusScan* is the same as ever, in the middle of the pack. The overhead of *VShield* is perhaps slightly larger than that of some of the other products, but not significantly so. Pleasingly, no false positives were registered against the Clean set. The only real gripe with the product concerned its sporadic (at best) detection of floppy disk changes. This problem has been noted before, but still persists.

Norman Virus Control v4.72 (31/8/99)

ITW Overall	100.0%	Macro	99.6%
ITW Overall (o/a)	100.0%	Standard	99.8%
ITW File	100.0%	Polymorphic	96.9%

Another impressive display from *Norman Virus Control* (*NVC*) earns the product its tenth VB 100% award. The majority of the misses can be accounted for by the samples of ACG.A from the Polymorphic set. Elsewhere, misses were few and far between – a handful of *Word* macro viruses (Ozwer.A,

Chack.AR and IIS.H) and a JavaScript file infected with VBS/First.C. It was pleasing to see similarly impressive results during the on-access tests, thanks to *NVC's* on-access scanner, *Cat's Claw*.

Sophos Anti-Virus v3.25 (31/8/99)

ITW Overall	100.0%	Macro	99.4%
ITW Overall (o/a)	99.7%	Standard	98.4%
ITW File	100.0%	Polymorphic	96.9%

A typically strong performance from *Sophos Anti-Virus* (*SAV*), although unfortunately not sufficient to claim the VB 100% award. *PowerPoint* files infected with O97M/Tristate.C were missed from the ItW set due to the failure of *InterCheck* (*SAV's* on-access component) to include *PowerPoint* files by default. To include such files (and any others deemed necessary), *InterCheck's* configuration file has to be edited manually.

As ever, *SAV* was one of the easy products to test, with perfect stability exhibited by both its on-demand and on-access components. The latter gives an overhead of approximately 100% when enabled, which is slightly less than that induced by some of the other products.

Symantec NAV v5.02.04 (27/8/99)

ITW Overall	100.0%	Macro	99.3%
ITW Overall (o/a)	100.0%	Standard	99.7%
ITW File	100.0%	Polymorphic	93.9%

As can be seen from the results, impressive detection rates were observed with *Symantec's Norton Anti-Virus* (*NAV*), and the product picks up its seventh VB 100% award.

The final product in this Comparative, *NAV*, behaved impeccably, just like *SAV* before it. It was perfectly stable throughout testing. In keeping with some of the other products featured in this review, *NAV* uses heuristics by default. Thankfully, the *Bloodhound* heuristics employed by *NAV* did not register any false positives during the speed and overhead tests.

The misses were due to ACG.A and ACG.B samples in the Polymorphic set, VBS/Happy in the Standard, and a handful of *Word 8* macro viruses together with PP97M/Vic.A in the Macro set.

Summary

In this, the first Comparative where on-access scanning is incorporated into the VB 100% award, eight products managed to make the grade. A number of others came close, but missed due to the simple product configuration issue of failure to scan sufficient file types.

Another Comparative first is the fact that all the submitted products sported an on-access scanner of some description – perhaps reflective of how dependent users are on them nowadays. The stability of the on-access scanners is perhaps an area of concern, however. Certainly, exposing the scanners to almost 20,000 infected files might not be a realistic situation, but even so, the lack of stability exhibited by a few of the products does not inspire confidence.

The final first in this Comparative is the inclusion of VBS viruses in the test-set. This was partly driven by the recent reports of VBS/Freelinks in the wild. Despite the fact that this virus made its first appearance at the start of July, only five of the 16 products tested managed to detect all three of the variants included in the tests. Perhaps the fact that the first of these variants is now officially on the October 1999 WildList will see VBS/Freelinks' detection finally being added to the remaining products – a few of which already have the necessary updates available from their Web sites.

Technical Details

Test Environment: Server: *Compaq Prolinea 590*, 90 MHz 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 98*. The workstations were rebuilt from image back-ups, and the test-sets were stored in a read-only directory on the server.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/Win98/199911/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.