COMPARATIVE REVIEW

In the Frame

It has been eight months since *VB* last published a comparative review of *Windows 95* scanners. At the beginning of 1997 there was a suspicion we may be running our first 'Which products best made the transition to *Windows 97*?' review, but the folk at Redmond have postponed our ability to run those tests for a few more months (and it will then be the 'transition to *Windows 98*' review).

As was remarked back in May, *Windows 95* and most of the products designed for it have reached a fair degree of stability and acceptance in the mainstream computer market, though many large corporate IT departments are clinging to *Windows 3.1* until making the move directly to *Windows NT*.

We received twenty packages in response to our call for products, including two new faces – *eSafe* being a souped-up and repackaged version of *EliaShim's ViruSafe* and *RAV*, from *GeCAD* in Romania, being completely new to *Virus Bulletin* tests (although the version number of 5.02a suggests it has a fair tradition in its home market). Most of the products provided the sort of initial user impression expected of contemporary *Windows 95* applications – good, easy to follow installation procedures that leave an uninstall option, progress indicators, browse buttons where they should be, context menu additions (scan drive/file/folder on right-click in Explorer) and the like. Seventeen of the twenty had a resident or on-access scanning component, but one of these could not be tested because it only detected viruses on execution of infected files and *Virus Bulletin* cannot test this detection mode.

Testing

As usual for *VB* comparatives, vendors were asked to supply the product they would sell to *Windows 95* user looking for virus protection. GUI-only anti-virus software would present a small problem in cases where *Windows 95* will not start and/or in the case of boot sector infections, where most products (rightly) refuse to disinfect the virus while it is active. The simple solution to these problems is to provide a DOS scanner for 'emergency use'. A few products take this a step further and provide their own 'emergency boot diskette'. Although these components are clearly very important should you need to resurrect an infected system, we focused solely on the 'main scanner', which in all but one case was a *Win32* GUI application.

In a break with *VB* tradition, the tests were run on three machines. Ostensibly identical, these were all built to the same specification with the same components and all hardware was configured identically (for specifications see the Technical Details box at the end of the review). Despite the machines supposedly being identical, all timed tests were run on just one of them. The operating system was installed and configured on one machine, the disk fully defragmented and free space on it filled with zeroes. A sector-level image was then made. This was implanted onto each of the other machines, where minor configuration changes were necessary (all three machines are on the test network, and thus needed different names and the like). Images were then made of the second and third machines' disks. Between installing each product for testing, the hard drive was completely rewritten from the appropriate image file, so each test started from the same point.

The common *VB* tests were run – speed (and propensity for false alarms) against the Clean test-set, speed against a clean and infected diskette, and virus detection. With the increasing use (and importance) of resident or on-access scanning, we tested the detection abilities of the products with such options. Lastly, we endeavoured to measure the performance overhead of on-access scanning.

Please note that except in the case of 100% scores and the ItW Boot test-set, taking the number of samples detected in a test-set and dividing by the total number of samples in that set can give a slightly different result from that reported. This is particularly true of the Polymorphic test-set. The results are based on a weighted calculation that corrects for the number of samples of each virus (and provides a bonus weighting for complete detection of a stem in the case of the Polymorphic test-set). A complete explanation of these calculations is available from the *VB* web site address given in the Technical Details section.

The test-sets used were updated slightly, relative to the previous comparative review. The most important changes reflected the modifications to the WildList, bringing the ItW sets up-to-date to August 1997 (the current WildList at product submission date).

On-access Tests

Both the on-access tests – detection and overhead – caused the reviewer considerable grief. Due to a range of problems across many of the products, the on-access detection tests were eventually cut back to just the In the Wild File and Macro test-sets (probably the two of most concern to our readers). We plan to run on-access detection tests of all test-sets in our next Win32 comparative (*NT* in March).

The detection tests were complicated enormously by several products not having a 'log only' option for their on-access scanner, or having one that did not work. The prospect of sitting through more than 15,000 virus detection dialog boxes, and pressing a key each time, was not very

	ItW Boot		ItW File		ItW Overall	Macro		Polymorphic		Standard	
	Number	%	Number	%	%	Number	%	Number	%	Number	%
Alwil AVAST32	90	100.0%	637	98.3%	98.9%	731	98.5%	12503	96.2%	799	100.0%
Command F-PROT Pro	90	100.0%	646	100.0%	100.0%	721	97.4%	7060	49.4%	709	91.7%
Cybec VET	87	96.7%	634	98.4%	97.8%	720	96.9%	12885	97.4%	782	98.0%
Data Fellows F-PROT Pro	87	96.7%	646	100.0%	98.9%	713	96.4%	7050	50.3%	709	91.7%
Dr Solomon's AVTK	89	98.9%	646	100.0%	99.6%	723	97.4%	12939	97.7%	799	100.0%
eSafe Protect	88	97.8%	646	100.0%	99.2%	721	97.4%	12632	91.1%	779	97.9%
Eliashim ViruSafe 95	88	97.8%	646	100.0%	99.2%	721	97.4%	12632	91.1%	779	97.9%
GeCAD RAV	77	85.6%	568	89.4%	88.1%	490	65.3%	12457	94.0%	747	93.3%
H+BEDV AntiVir/95	87	96.7%	602	93.1%	94.3%	734	98.5%	9607	71.8%	714	92.7%
IBM AntiVirus	88	97.8%	646	100.0%	99.2%	736	99.5%	12500	96.2%	799	100.0%
Intel LANDesk Virus Protect	81	90.0%	619	95.7%	93.7%	646	87.2%	11762	87.1%	765	96.3%
iRiS AntiVirus	88	97.8%	645	99.7%	99.1%	733	98.6%	12480	95.1%	793	99.3%
KAMI AVP	89	98.9%	643	99.6%	99.3%	740	100.0%	12806	97.0%	799	100.0%
McAfee VirusScan	89	98.9%	646	100.0%	99.6%	728	98.5%	12941	98.7%	779	98.4%
Norman ThunderByte	90	100.0%	646	100.0%	100.0%	729	98.6%	12996	98.1%	789	99.0%
Norman Virus Control	90	100.0%	646	100.0%	100.0%	729	98.6%	13000	100.0%	782	98.7%
Sophos SWEEP	90	100.0%	646	100.0%	100.0%	732	99.0%	13000	100.0%	797	99.7%
Stiller Integrity Master	85	94.4%	574	90.8%	92.1%	609	81.9%	4582	30.3%	595	81.5%
Symantec Norton AntiVirus	89	98.9%	640	99.4%	99.2%	731	98.5%	11501	87.5%	784	99.0%
Trend Micro PC-cillin	86	95.6%	632	97.5%	96.9%	736	99.5%	12383	93.6%	769	96.5%

appealing. Fortunately, the old trick of wedging the Enter key down looked as if it would suffice. But it was not to be. Some of the products that insist on presenting a warning do so with a system-modal dialog box, or a VxD blue-screen warning. These screens have to ‘see’ a key press and release before yielding, so the jammed down Enter key was not a runner. We understand there can be good reasons not to suppress such warnings, but there are situations where you do not want your machine to stop dead even though your anti-virus software has found something to warn you about. A small, key-pressing robot to get around such problems in future tests might have to be added to the *VB* test-equipment armoury.

The on-access overhead tests were performed in much the same way as in the most recent *NT* comparative (*VB*, September 1997, p.10) – copying 200 executable files from the Clean test-set from one local directory to another ten times and averaging the copying times. A slight modification was made because *Windows 95* file I/O performance seems much more variable than *NT’s*. To reduce the effect of this in the results, the slowest and fastest test of the ten runs were removed from each condition’s results before calculating baseline times and overheads. We are still considering the design of more realistic overhead tests and stress that the results presented are indicative of a somewhat unusual activity for a ‘typical workstation’.

Alwil AVAST32 v7.70 22 Aug 1997

ItW Boot	100.0%	Macro	98.5%
ItW File	98.3%	Macro on-access	n/t
ItW File on-access	n/t	Polymorphic	96.2%
ItW Overall	98.9%	Standard	100.0%

Little seems to have changed since the last review, but as *AVAST32* performed well in the past, this is not a bad thing. The In the Wild Boot detection problems mentioned in the previous *Windows 95* comparative have clearly been fixed, with *AVAST32* turning in an unbeatable 100% on this test-set. ItW File detection is slightly down on recent results – this is solely due to missing three of the *Word 8* macro viruses (Appder.A, Kompu.A and Wazzu.C) in the test-set. The latter virus and two fairly new ones (at the time of testing), Header.A and Mess.A, prevented a perfect score against the Macro test-set, and 497 Cordobes.3334 samples were missed in the Polymorphic test-set.

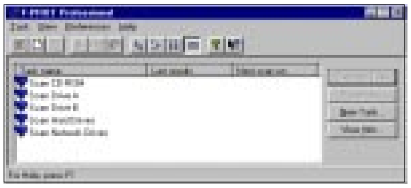
AVAST32 has an on-access scanner, but it only detects on execution and not on file open or other kinds of access. Consequently, this feature could not be tested. As the overhead test only involves executing the timing program and XCOPY ten times each, it seemed misleading to run *AVAST32* through this test.

High speed is not something *AVAST32* is noted for; in fact, it was slowest on the hard disk tests in the current round-up, taking six to eight times as long to scan the Clean test-set as its nearest rival. This may seem terrible, but it is a design feature. The developer claims that the on-demand scanner runs in a low-priority thread, and an informal test suggests that other applications do not slow down significantly while an on-demand scan grinds away in the background. Floppy scanning was also slow, placing *AVAST32* second-last on both diskette tests. Unfortunately, two false positives were registered against the Clean set.

Command F-PROT v3.00 18 Aug 1997

ItW Boot	100.0%	Macro	97.4%
ItW File	100.0%	Macro on-access	97.4%
ItW File on-access	100.0%	Polymorphic	49.4%
ItW Overall	100.0%	Standard	91.7%

With 100% In the Wild Overall detection, *Command F-PROT Professional* is one of four products to earn a VB 100% award in this review. This excellent ItW performance was maintained by its on-access scanner. Missing the two newer *Word* macro viruses Header.A and Mess.A and failing to handle *Excel* viruses other than XM/Laroux.A resulted in 97.4% detection of the Macro test-set.

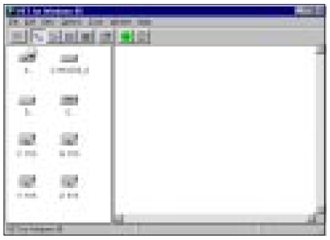


Such effective detection does not extend to the Standard and Polymorphic test-sets. In fact, a score below 50% on the latter must be a little worrying. Despite being supplied with a more up-to-date scan string set than came with the *Data Fellows F-PROT Professional*, *Command's* version missed one SatanBug.5000.A sample, denying it the 'bonus' for that stem. Thus, *Command F-PROT* received a lower rating on the Polymorphic test-set than the *Data Fellows* version, even though it detected a handful more viruses (amongst the Alive.4000 samples).

Speed and overhead are an interesting trade-off with this product. At the slower end of the fastest third of scanners tested, and twice as fast as about half of the muster, you will probably not be disappointed in its on-demand performance. It also returned the fastest clean diskette scan time, which increased by half on the infected diskette test. However, its on-access overhead of about 50% puts it in the bottom third for this test, with about half the products providing noticeably less overhead. No false positives were detected in the Clean test-set.

Cybec VET v9.5.1

ItW Boot	96.7%	Macro	96.9%
ItW File	98.4%	Macro on-access	96.9%
ItW File on-access	98.4%	Polymorphic	97.4%
ItW Overall	97.8%	Standard	98.0%



Traditionally one of the faster products, *Cybec's* offering came in third fastest on the Clean set, and it correctly found no viruses there. *VET* missed three samples from the ItW Boot – the same three that caused so many products problems in the recent *NT* comparative. Interestingly, *VET* for *NT* detected those samples, which shows there is more to writing a *Win32* anti-virus program than bolting a flash GUI onto an existing detection engine. The HLLP.5850.C and .D samples added in the August WildList update, and the *Word 8* form of Wazzu.C denied *VET* 100% on the ItW File test. On-demand detection rates around 97-98% against *VB* test-sets are typical of recent *VET* performance.

In keeping with its speedy reputation, *VET* was third and fourth fastest, respectively, on clean and infected diskette scanning. An overhead of 20% on the 'read and write' condition is still better than many (nine in this test), but it is probably starting to be noticeable.

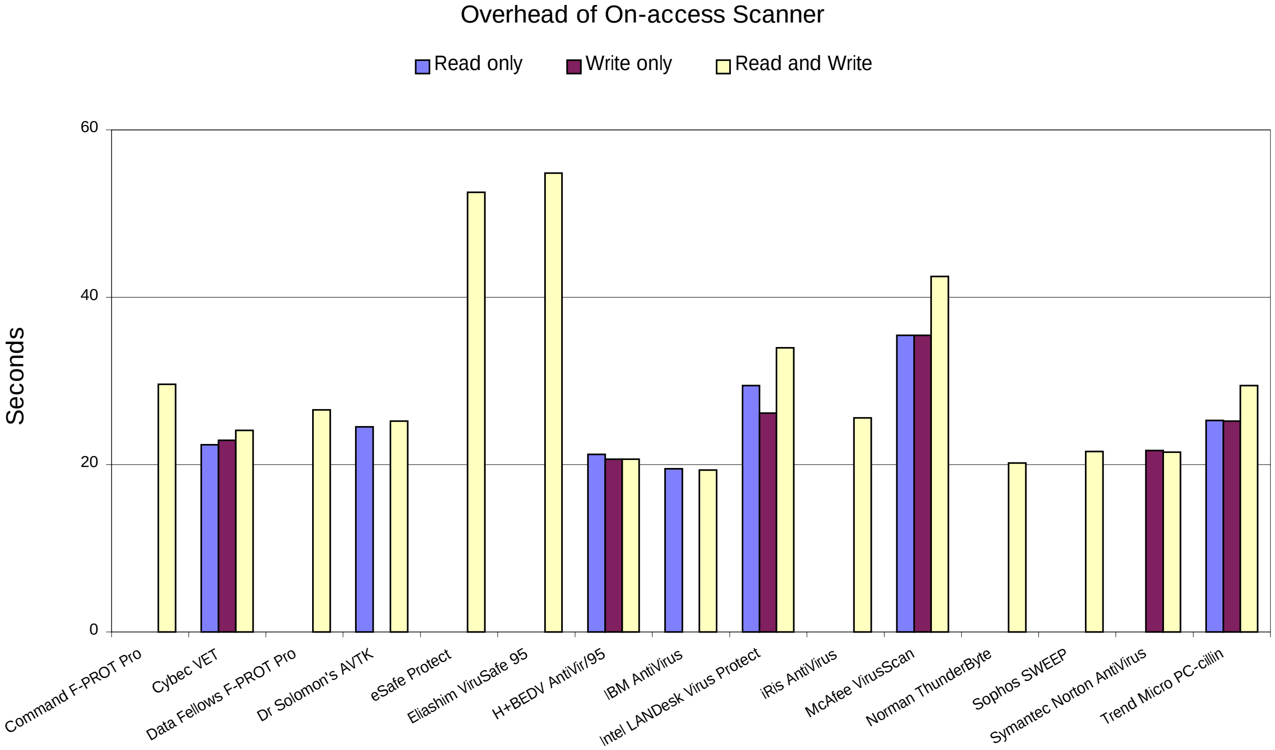
	ItW File on-access		Macro on-access		Hard Drive Speed		Clean Diskette Speed		Infected Diskette Speed		False Positives
	Number	%	Number	%	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	Scan time (min:sec)	Data rate (KB/s)	
Alwil AVAST32	n/t	n/t	n/t	n/t	88:48	100	1:05	15	1:12	16	2
Command F-PROT Pro	646	100.0%	721	97.4%	4:29	1986	0:21	46	0:38	31	0
Cybec VET	634	98.4%	720	96.9%	3:13	2767	0:25	39	0:29	41	0
Data Fellows F-PROT Pro	632	97.1%	707	94.9%	5:48	1535	0:27	36	0:43	27	0
Dr Solomon's AVTK	646	100.0%	740	100.0%	3:36	2473	0:32	30	0:59	20	0
eSafe Protect	638	98.9%	709	95.9%	4:10	2136	0:21	46	0:24	49	9
Eliashim ViruSafe 95	638	98.9%	709	95.9%	4:49	1848	0:22	44	0:25	47	9
GeCAD RAV	n/a	n/a	n/a	n/a	10:55	815	0:42	23	1:06	18	31
H+BEDV AntiVir/95	574	89.1%	670	89.7%	7:47	1144	0:34	29	0:40	30	6
IBM AntiVirus	504	78.9%	732	99.0%	2:05	4273	0:29	34	0:33	36	0
Intel LANDesk Virus Protect	613	95.2%	646	87.2%	10:58	812	1:19	12	1:40	12	0
iRiS AntiVirus	645	99.7%	694	94.0%	8:52	1004	0:34	29	0:39	30	16
KAMI AVP	n/a	n/a	n/a	n/a	10:16	867	0:56	17	0:46	26	0
McAfee VirusScan	646	100.0%	728	98.5%	10:26	853	0:46	21	0:54	22	0
Norman ThunderByte	646	100.0%	729	98.6%	3:05	2887	0:25	39	1:10	17	1
Norman Virus Control	n/t	n/t	725	98.1%	5:45	1548	0:41	24	0:58	20	0
Sophos SWEEP	640	99.1%	729	98.6%	5:15	1696	0:36	27	0:32	37	0
Stiller Integrity Master	n/a	n/a	n/a	n/a	4:13	2111	0:29	34	0:42	28	1
Symantec Norton AntiVirus	640	99.4%	739	99.5%	5:13	1706	0:41	24	0:57	21	0
Trend Micro PC-cillin	632	97.5%	736	99.5%	11:12	795	0:45	22	0:59	20	0

Data Fellows F-PROT v3.00 17 June 1997

ItW Boot	96.7%	Macro	96.4%
ItW File	100.0%	Macro on-access	94.9%
ItW File on-access	97.1%	Polymorphic	50.3%
ItW Overall	98.9%	Standard	91.7%

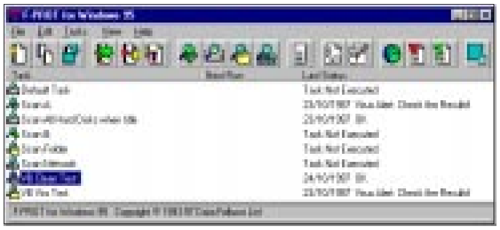
A perfect score against the In the Wild File test-set is always encouraging, but missing three In the Wild Boot viruses takes the gloss off this somewhat. Again, it was samples exhibiting the BPB problem that has been mentioned in the two previous *NT* comparatives. Soon after this product was submitted for review, *Data Fellows* informed *Virus Bulletin* that it had rectified the BPB problem with its *NT* product. Hopefully *Data Fellows* is also addressing this issue in its *Windows 95* product.

Data Fellows provided the review copy on CD-ROM, but did not supply an updated scan string set. As the CD was the June release, it seemed unlikely its results would be quite as good as *Command's* despite both products being based on the same scanning engine. Despite this, or perhaps highlighting the depth of experience and research behind the scanning engine, detection of the ItW File set matched, but perhaps not surprisingly, *Data Fellows F-PROT* scored a little lower on the Macro test-set.



The on-access tests returned slightly poorer performances than the on-demand ones. Fourteen ItW samples were missed in this test (all of the *Word 8* and *Excel 8* samples in the ItW set), as were an additional six samples in the Macro test-set (four of W97M/Nightshade and one each of W97M/Wazzu.A and .C).

On-demand scanning speed and on-access overhead were both in the middle of the pack, but quite acceptable. Floppy disk scanning speed ranked slightly higher, but was nothing to write home about. No false positives were reported against the Clean test-set. The test machine's performance was unreliable with the *Data Fellows* product installed, locking-up occasionally and trapping many exceptions. Hopefully these stability issues will have been addressed in later releases.



Dr Solomon's AVTK v7.74 23 June 1997

ItW Boot	98.9%	Macro	97.4%
ItW File	100.0%	Macro on-access	100.0%
ItW File on-access	100.0%	Polymorphic	97.7%
ItW Overall	99.6%	Standard	100.0%

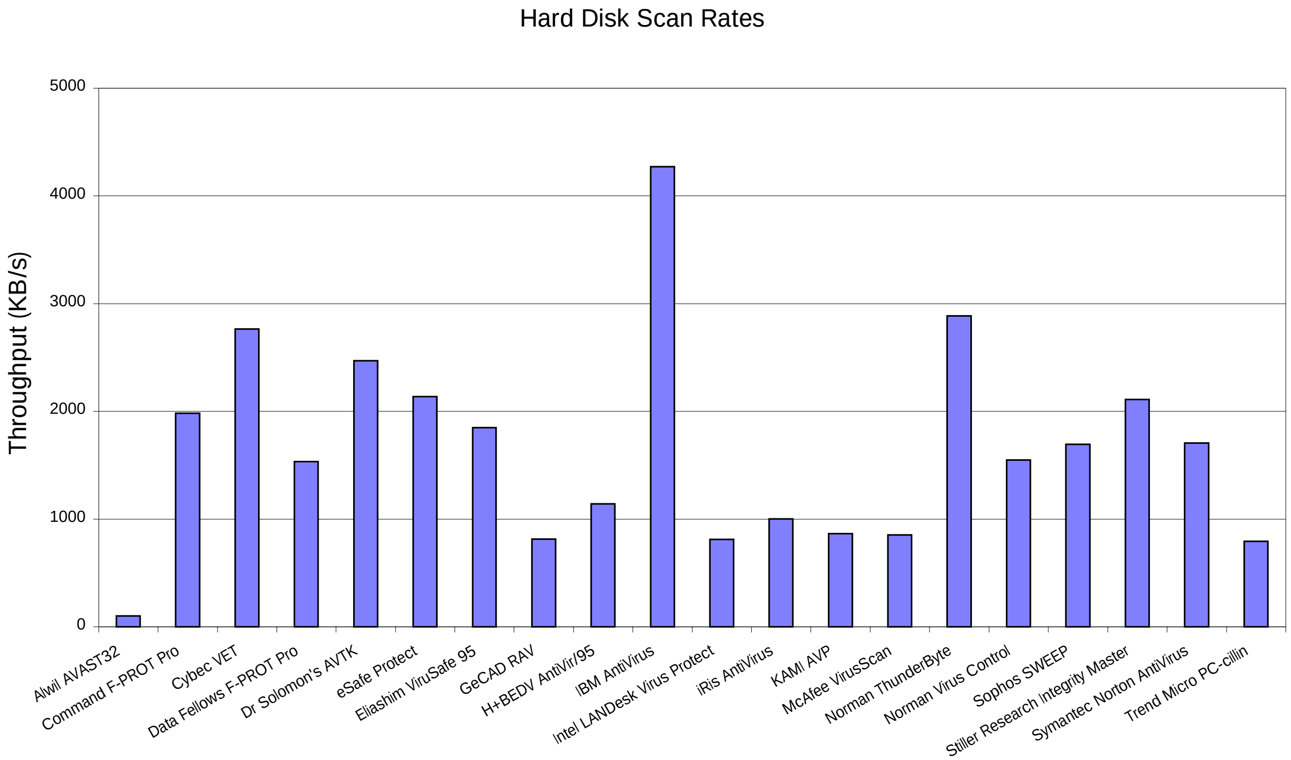
Submitting what, at the time, was a slightly outdated version of their software might have been what stood between *Dr Solomon's AVTK* scoring 100% ItW Overall and missing it by the single sample of the boot infector Moloch. However, the breadth and depth of *AVTK's* detection capability is seen in the fact that, despite its age, it detected 100% of both the Macro and Standard test-sets, and only missed 61 samples in the Polymorphic test-set.

Although not renowned as a speedster, the *AVTK* had fourth highest throughput scanning the Clean test-set, but fell fairly much mid-range on the diskette tests. Its 25% on-access overhead might not upset, but there are products with a lower impact. It was interesting that the on-access scanner detected 100% of the Macro set, bettering the on-demand scanner! Regardless, it was one of only two products to achieve 100% on this set. On-access detection of the ItW File set stayed at 100%.

The *AVTK* interface still does not 'feel' very much like a *Windows 95* program. There is not much else to say – *AVTK* gave its typically high detection and no false positives.

eSafe Protect v1.02 28 Aug 1997

ItW Boot	97.8%	Macro	97.4%
ItW File	100.0%	Macro on-access	95.9%
ItW File on-access	98.9%	Polymorphic	91.1%
ItW Overall	99.2%	Standard	97.9%



The first of the two newcomers to *VB* tests, *eSafe Protect* proclaims itself as ‘the original anti-vandal software’. A product of *eSafe Technologies*, a division of *EliaShim*, *eSafe Protect* is based on the same virus scanning engine as *EliaShim’s ViruSafe* (see below) but adds ActiveX and Java malware detection capabilities, and behaviour blocking. These were not tested in this review.

The on-demand scanner module looks very like *ViruSafe* with a different colour scheme and ancilliary graphics. However, the actual *eSafe* interface is quite ‘exciting’ (for lack of a better word). With its animations, levers and dials it would not have looked out of place on a hand-held, flip-top, hi-tech gadget in a recent movie. Although not the version submitted for review, most *VB* readers would probably be more interested in the Enterprise version, which is claimed to be geared to corporate LAN/Intranet use. *eSafe Protect’s* performance was essentially identical to *ViruSafe’s*, discussed below.

EliaShim ViruSafe 95 v2.1 28 Aug 1997

ItW Boot	97.8%	Macro	97.4%
ItW File	100.0%	Macro on-access	95.9%
ItW File on-access	98.9%	Polymorphic	91.1%
ItW Overall	99.2%	Standard	97.9%

As explained above, *ViruSafe* and *eSafe* both use *EliaShim’s* scanning engine. As the same version and scan string set were supplied with both, it is not surprising they obtained the same results – in fact, it would be notable if they had not done so.

Missing Moloch and Hare.7750 on the ItW Boot test-set prevented both scanners from scoring 100% ItW Overall. On-access scanning missed the two *Excel* macro viruses in the ItW File set (XM/ and X97M/ versions of Laroux.A). It seemed this may have been because XL? was not in the default extension list for the on-access scanner, but adding it did not change things. Similarly, when testing the on-access component against the Macro set, both products missed four samples of each of three Excel macro viruses that were detected by the on-demand scanner. *EliaShim’s* detection rate of the Polymorphics climbed slowly through 1997 and it is pleasing to see this improvement continue.

Speed and overhead are something of a mixed-bag with the *EliaShim*-engined products. Both products returned very respectable throughputs around the 2100 KB/s mark in on-demand scanning (fifth-equal) and the fastest diskette scan speeds, but quite poor on-access overhead results of about 150% (the highest overheads in our tests).

GeCAD RAV v5.02a 30 Aug 1997

ItW Boot	85.6%	Macro	65.3%
ItW File	89.4%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	94.0%
ItW Overall	88.1%	Standard	93.3%

As mentioned earlier, *RAV* is the second of two newcomers to *VB* tests. The developers were anxious to see how their product fared against the *Virus Bulletin* test-sets and seemed to view submitting their product to our testing as a development opportunity. Although *GeCAD* has primarily targeted *RAV* at the Romanian market, the test copy was supplied as boxed packages with English versions of the software (but Romanian manuals).

RAV was one of the few products tested that did not use one of the common installation toolkits (most products tested used *InstallShield*), but it installed easily and cleanly, apparently doing everything 'right'. I found the lack of accelerator keys frustrating in places and the very roundabout manner of executing a diskette scan was frustrating. This, combined with the lack of a 'repeat' or 'multi' option for diskette scanning would be enough to deter anyone from scanning a modest number of diskettes (say a pocketful), let alone ninety. This gripe applies fairly equally to several other products whose design seems to discourage diskette scanning. With the growing use of on-access scanning the need to bulk scan a pile of diskettes may be falling off, but the need would arise should an infection become widespread (especially if it were a boot infector).

RAV employs a combination of known-virus scanning and heuristic analysis techniques and these helped it score favourably on the Polymorphic and Standard test-sets. It did not fare quite so well on the ItW sets. However, detecting 88.1% ItW Overall in the first showing of a product that has focused on a regional market is an encouraging start. The developers admitted that macro virus detection was *RAV's* weak spot, and they claimed to be working on improving this. Given this warning, it was not surprising that *RAV's* poorest detection result was against the Macro test-set.

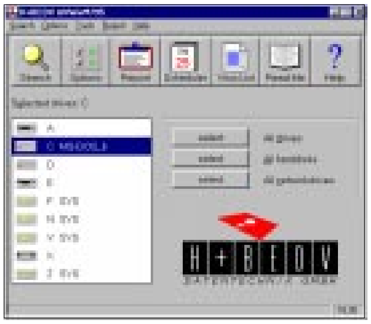
No speed leader, *RAV* was one of five products with a throughput on the Clean set of around 800 KB/s. A couple of products were slower, but over half were notably quicker. Similar comments apply to diskette scanning speed, but with an appropriately lower data rate (around 20 KB/s). Some work needs to be done tightening up the heuristic decision mechanism, as *RAV* claimed to find 31 likely viruses in the Clean set. The developers are working on a resident scanner, but this was not shipping at test time.

H+BEDV AntiVir/95 v1.02 22 Aug 1997

ItW Boot	96.7%	Macro	98.5%
ItW File	93.1%	Macro on-access	89.7%
ItW File on-access	89.1%	Polymorphic	71.8%
ItW Overall	94.3%	Standard	92.7%

A dramatic improvement in ItW Boot detection, compared with recent *VB* reviews, put *H+BEDV's* ItW Overall score back into the mid-nineties. A detection rate of 98.5% against the Macro test-set is a good result, and an encouraging improvement compared to *H+BEDV's* result against this test-set in the most recent NT comparative. It is pleasing to see *AntiVir's* gradual improvement against the other test-sets still continues.

AntiVir/95's on-demand performance was middle of the pack on both the hard disk and diskette speed tests, but this is admirably compensated for by an overhead of only 5%. The on-access scanner does not detect all of the viruses the on-demand one does, but its low overhead is fairly constant, regardless of configuration. Reporting six viruses in the Clean set puts a kink in the results however.



IBM AntiVirus v3.0f

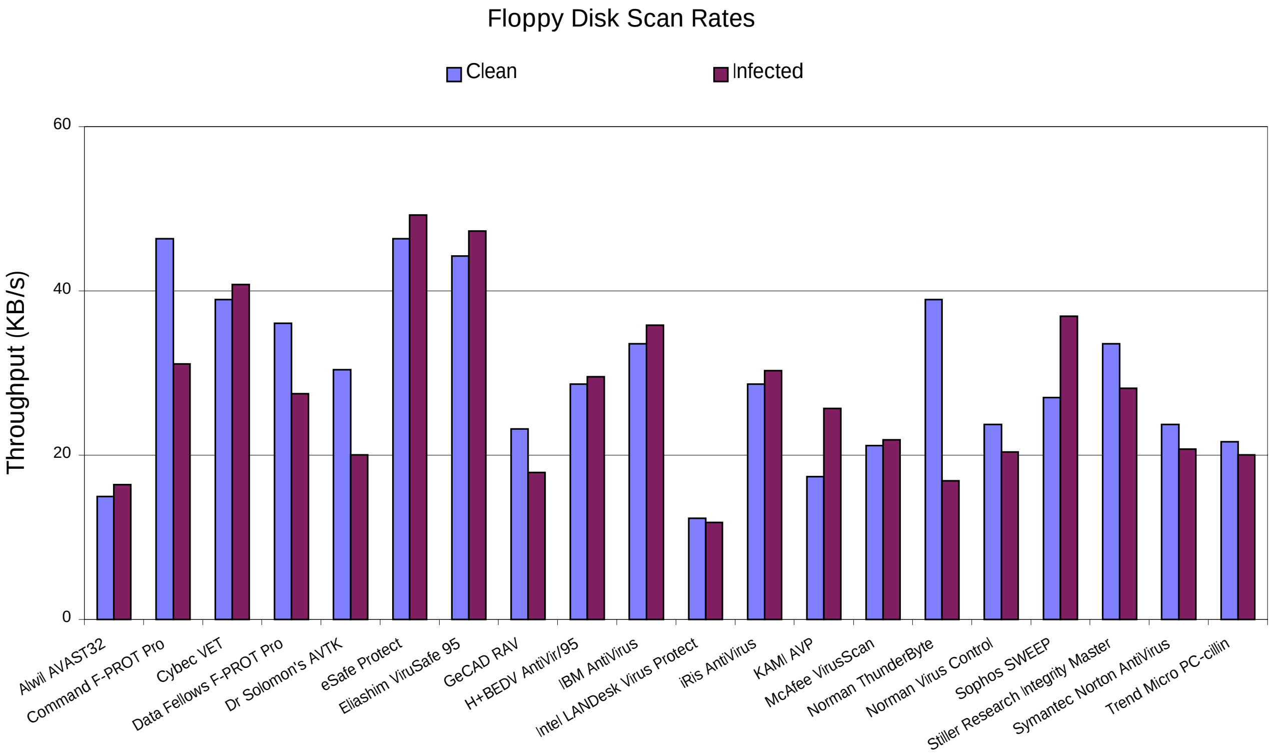
ItW Boot	97.8%	Macro	99.5%
ItW File	100.0%	Macro on-access	99.0%
ItW File on-access	78.9%	Polymorphic	96.2%
ItW Overall	99.2%	Standard	100.0%

The boot virus test-set continued its record of causing problems for Win32 scanners in denying *IBM AntiVirus* (*IBMAV*) a 100% ItW Overall score. Apart from missing Michelangelo.A and MISiS on the In the Wild Boot test, *IBMAV* missed only two other viruses from the rest of the *Virus Bulletin* test-sets – four samples of the new WM/Header.A and the Cryptor.2582 stem from the Polymorphic set. This is an impressive result.

The on-access component of *IBMAV*, called System Shield, does not provide the same detection as the on-demand scanner. Four samples of the relatively new *Word* virus (WM/Mess.A) were missed by System Shield, as were 142 samples (covering 38 viruses) from the ItW File set. By default, System Shield is configured to intercept 'execution'. File-open calls count as 'execution' for OLE2 files (*Word* and *Excel* documents), but a

To check your system for viruses now

For Help, press F1



load-and-execute is required for it to detect program viruses. To run a meaningful test without the risk of executing infected programs, System Shield was set to monitor all file accesses. Interestingly, the warning that this option may slow the machine down was unduly pessimistic, as both System Shield conditions resulted in slightly faster, rather than slower performance!

Another notable *IBMAV* result was its scanning speed. *IBMAV* uses integrated checksumming. After scanning a file the first time and ensuring it is not infected, *IBMAV* records a partial checksum of it. This is quickly calculated when the file is accessed again, compared with the stored value, and if the two match, the file is not be re-scanned. This makes subsequent scans of files that seldom change (most programs) very fast. Our current tests do not address performance issues with regularly changing files, such as *Word* documents.

The scan speeds presented here are based on the second scan of the Clean test-set – the first scan took almost exactly eight times as long, and would have placed *IBMAV* second slowest. This sort of scan time will be experienced on an initial install and subsequent scan string updates. *IBMAV* was in the top third of performers on the diskette speed tests, and recorded no false positives.

Intel LANDesk Virus Protect v5.0 VPN 317

ItW Boot	90.0%	Macro	87.2%
ItW File	95.7%	Macro on-access	87.2%
ItW File on-access	95.2%	Polymorphic	87.1%
ItW Overall	93.7%	Standard	96.3%

Showing a large improvement against the Standard test-set (from 71.4% in May 1997), *Intel LANDesk Virus Protect* is holding its own against the Polymorphic and Standard test-sets, but has slipped somewhat against the In the Wild Boot and File sets. Despite an improvement against the Macro test-set (compared to its *NT* stablemate in the September 1997 comparative), a detection rate of 87.2% on this test is likely to be considered too low by many.

Trailing the pack on diskette scan rates and falling in the group of five with approximately 800 KB/s on the hard drive throughput test, you would be unlikely to choose this product for its speed.

Ranging from 30% to 70%, depending on configuration, *Virus Protect's* on-access overhead is not the most daunting in the test, but falls in the bottom third of products in this regard. It detected the same viruses from the In the Wild File test-set using either method, but its on-access component missed six samples from the Macro test-set that the on-demand scanner detected.

LANDesk® Virus Protect 5.0
Client for Windows 95, Windows NT

Copyright © 1997 by Intel Corporation.
All rights reserved.

Version information
Scan engine: [illegible]
Virus pattern file: 317
File date: [illegible]

Having the unusual option to set scanning exclusions by virus name, the cynical might assume that *Virus Protect* has a problem with false positives (what other good reason could there be for this option?), but there was no evidence of this in testing against the *VB* Clean test-set.

iRiS AntiVirus v22.01 3 Sep 1997

ItW Boot	97.8%	Macro	98.6%
ItW File	99.7%	Macro on-access	94.0%
ItW File on-access	99.7%	Polymorphic	95.1%
ItW Overall	99.1%	Standard	99.3%

Still striving for a 100% In the Wild Overall score, *iRiS AntiVirus* missed by two boot sector viruses and one of two No_Frills_Dudley samples in the ItW File set. The product's failure to generate a useful log file regardless of which combination of settings was tried nearly resulted in it recording a 'did not complete' in the on-demand Macro test. A patient afternoon's investigation uncovered the fact that the program was hanging when trying to scan the WM/Rapi.B sample. Removing this from the test set (and counting it as a miss – only fair for all that work!) showed an otherwise good result of 98.6%. A small improvement is noted against the Polymorphic set.

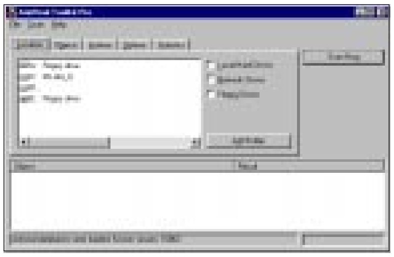
The on-access component achieves the same detection rate against the In the Wild File set as the on-demand scanner, but misses 39 samples from the macro set that are detected on-demand. The on-access overhead of around 27% puts it in the company of such products as *AVTK*, *Data Fellows F-Prot* and *VET*. Hard disk and floppy scanning speeds were middle of the pack. *iRiS AntiVirus* raised sixteen false alarms against the *VB* Clean test-set.

KAMI AVP v3.0.114 2 Sep 1997

ItW Boot	98.9%	Macro	100.0%
ItW File	99.6%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	97.0%
ItW Overall	99.3%	Standard	100.0%

Returning excellent detection on all test-sets is the expected behaviour of *AVP*. While the detection rates lapsed slightly as the developers focused on producing non-DOS versions of the program, it looks as if the job of recovering from the slipping detection rate is all but complete. *KAMI's* scanner was one of only two to post 100% detection against the Macro test-set. As for scanning speed, *AVP* was one of the 800 KB/s group and was third slowest on the clean diskette test. It was markedly faster on the infected diskette, however, falling squarely in the middle of the field on that test.

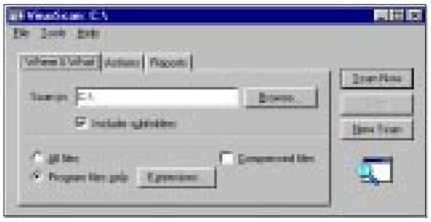
The interface does not seem to have changed much since the previous *Windows 95* comparative, however, with the full version you now get an emergency boot disk. There is no on-access scanning component to *AVP*.



McAfee VirusScan v3.1.1 19 Aug 1997

ItW Boot	98.9%	Macro	98.5%
ItW File	100.0%	Macro on-access	98.5%
ItW File on-access	100.0%	Polymorphic	98.7%
ItW Overall	99.6%	Standard	98.4%

Compared to its excellent showing in the previous *Windows 95* comparative, overall detection has slipped very slightly, but a product detecting 100% of the ItW File set and more than 98% on all test-sets cannot be ignored. All that prevented *VirusScan* scoring 100% ItW Overall was Stoned.Daniela.



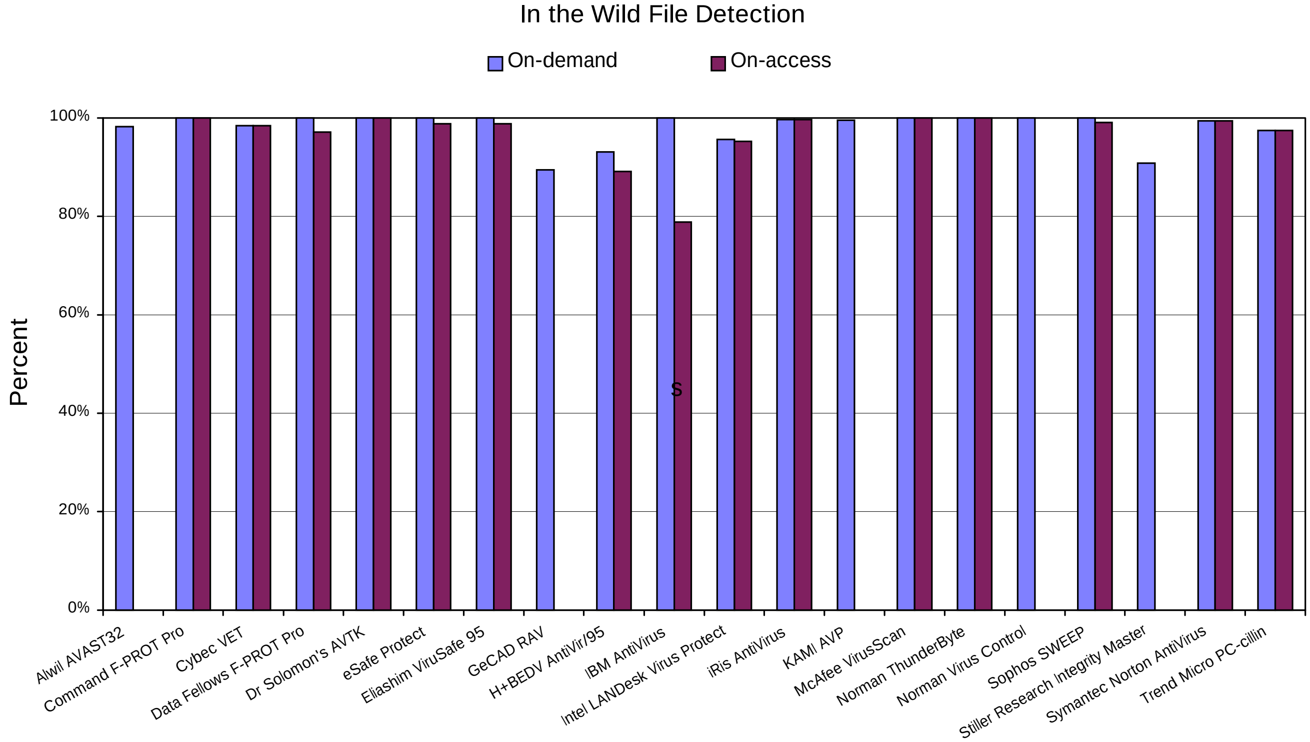
VirusScan's on-access scanner matches detection of its on-demand one – a design goal one would have thought easy to achieve, but which only three other products achieved. Maybe it is naive to expect that on-access and on-demand detection rates should match?

VirusScan's speed is towards the bottom of the field now, being one of the approximately 800 KB/s scanners on the hard disk test and 20 KB/s scanners on diskettes. It correctly failed to find any viruses in the Clean test-set. Its on-access scanner introduces a higher overhead than all others tested except those based on the *EliaShim* engine. As we have commented before, the elegantly simple interface, similar to Find Files makes the on-demand scanner very easy to use, which is an attraction of this product.

Norman ThunderByte v8.03 1 Sep 1997

ItW Boot	100.0%	Macro	98.6%
ItW File	100.0%	Macro on-access	98.6%
ItW File on-access	100.0%	Polymorphic	98.1%
ItW Overall	100.0%	Standard	99.0%

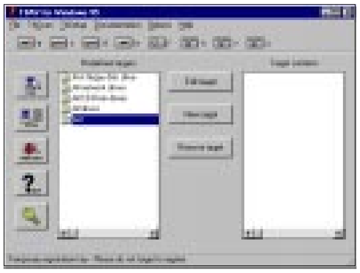
Despite its relatively poor showing in the previous *Windows 95* review, *Norman ThunderByte Virus Control* (whew – let's call it *NTVC*) is a product almost expected to produce a string of



100% scores, and it did not disappoint on this outing. *NTVC* is the second of four products in this review to attain a 100% ItW Overall rating, hence earning a VB 100% award. The macro viruses missed were the four samples of the relatively new WM/Header.A and WM/Mess.A, and three of the XM/Robocop.A samples.

NTVC's on-access component is either on or off, and is claimed to monitor all file I/O. This is not enabled by default. The performance impact of enabling this option was very low, however, returning a probably imperceptible 0.8% overhead. The File I/O Monitor returned the same detection results against the ItW File and Macro test-sets, as did the on-demand scanner.

An interesting feature of *NTVC* is the scheduler that runs background scans of your hard drive(s) at preset intervals. Renowned for its speed, it was not surprising that *NTVC* had the second highest throughput when scanning the Clean test-set. This was tarnished somewhat by it finding one false positive in the set.



Norman Virus Control v4.20 28 Aug 1997

ItW Boot	100.0%	Macro	98.6%
ItW File	100.0%	Macro on-access	98.1%
ItW File on-access	n/t	Polymorphic	100.0%
ItW Overall	100.0%	Standard	98.7%

Another *Norman Data Defense Systems* product, *NVC's* recent test history suggested it should perform as well as *NTVC*. As the third recipient of a VB 100% award, it was not to disappoint. A low score of 98.1% against the Macro test-set (with the on-access component) would be the envy of most developers, and *Norman's* consistently high performance on our tests is a credit to their research and development efforts.

NVC's scanning speed is in the middle of the pack on the hard drive test and it places a little lower on the diskette test. The on-access scanner was only tested against the Macro set and the macro viruses from the ItW File set (the latter result is not in the results table).

The on-access protection provided with *NVC* is somewhat different from that of most other products. It consists of several components. Cat's Claw is a 'traditional' on-access scanner that only knows about macro viruses. The Smart Behaviour Blocker only intercepts load-and-execute calls and could not be tested (see the discussion of this in the section on *Alwil's AVAST32*). Cat's Claw missed the *Word 6/7* virus Hiac.A and the DOT form of Concept.J from the ItW File set, and apart from the samples the on-

demand scanner missed, all Swlabs.G samples from the Macro set. As none of the files that are copied around in the overhead test were of DOC or XLS type, it seemed publishing an overhead test, in which Cat's Claw would have been all but idle, would be misleading.

Sophos SWEEP v3.01a 1 Sep 1997

ItW Boot	100.0%	Macro	99.0%
ItW File	100.0%	Macro on-access	98.6%
ItW File on-access	99.1%	Polymorphic	100.0%
ItW Overall	100.0%	Standard	99.7%

The fourth and final VB 100% award in this review goes to *Sophos' SWEEP*. Showing form similar to recent tests, *SWEEP* was one of only three products to detect 100% of the samples in three of the five *VB* test-sets (*Dr Solomon's AVTK* and *Norman Virus Control* being the others).

Somewhat surprisingly, the on-access component detected slightly fewer viruses in the ItW File and Macro tests. On examination, the misses were all DOC forms of *Word 8* macro viruses.

SWEEP's scanning speed is middle of the pack on both hard drive and diskette tests, although its infected diskette scan was noticeably faster than its clean diskette scan. The high detection rate is coupled with a low on-access scanner overhead of around 10%. As one would hope, no viruses were reported in the Clean test-set.

Stiller Research Integrity Master v3.21a

ItW Boot	94.4%	Macro	81.9%
ItW File	90.8%	Macro on-access	n/a
ItW File on-access	n/a	Polymorphic	30.3%
ItW Overall	92.1%	Standard	81.5%

It should come as no surprise that *Stiller Research* submitted their DOS-based product for review. The integrity checking part of *Integrity Master* is well-regarded, and apart from the user-interface 'niceties', there is probably no compelling reason to implement a GUI version of the product. That said, this review focuses on virus scanning and *Integrity Master* looks somewhat odd in the line-up.

The first stage of installing an integrity management system is usually to confirm the integrity of the things to be managed – it is generally not desirable to ensure the integrity of something that has already been compromised! Thus, *Integrity Master* includes a virus scanner, which we tested. A score of 92.1% In the Wild Overall is disappointing, given the significance of the task *Integrity Master's* scanner is charged with. One would especially hope that all boot viruses thought to be in the wild would be detected.

That said, the flip side is (at least for file infectors) that a good integrity checker should spot any modifications due to subsequent infections from a virus that was missed by the pre-install scan. However, you may have to obtain another scanner or wait for *Stiller Research* to get an update to you to detect the source of these infections. Similar back-and-forward claims could be made about misses on any of the other test-sets.

Hard disk scanning speed is quite acceptable, ranking approximately a third of the way through the list. *Integrity Master* placed about mid-field on the diskette scanning tests, being a little faster on the clean diskette than on the infected one. Unfortunately, it also registered one false positive against the Clean test-set.

Symantec Norton AntiVirus Build 26J

ItW Boot	98.9%	Macro	98.5%
ItW File	99.4%	Macro on-access	99.5%
ItW File on-access	99.4%	Polymorphic	87.5%
ItW Overall	99.2%	Standard	99.0%

The software submitted for review was a pre-release copy of the eventual v4.0. It seemed fully functional except that the About option on the Help menu did nothing. The test results are interesting, showing slight slippage on both In the Wild test-sets.

More importantly, however, *Norton AntiVirus* (*NAV*) showed excellent gains against the Standard test-sets and a small improvement on the Macro test. These improvements are in no small part attributable to the inclusion of *Symantec's* fancifully-named heuristic code analyser, Bloodhound (the report files contained many instances of 'infected with

Select the drives you wish to scan, then click Scan Now.

the Bloodhound.ResCOM virus' and the like). Bloodhound did not significantly improve things against the Polymorphic test-set.

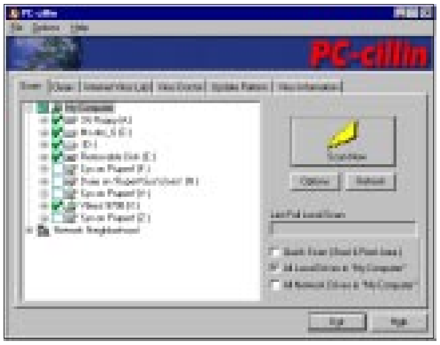
The on-access component detected slightly more macro viruses than the on-demand scanner, finding the four samples of both Word 6/7 viruses NJ-WMDLK1.A and Spiral.A. *NAV's* scanning speed was about middle of the pack on both the hard disk and diskette tests. On access overhead of 10% certainly puts *NAV* in the interesting part of the spectrum if system performance is important to you. It is encouraging that inclusion of Bloodhound's heuristics did not result in *Norton AntiVirus* reporting any false positives in the Clean set.

Trend Micro PC-cillin v3.00 VPN 323

ItW Boot	95.6%	Macro	99.5%
ItW File	97.5%	Macro on-access	99.5%
ItW File on-access	97.5%	Polymorphic	93.6%
ItW Overall	96.9%	Standard	96.5%

Evolving to major version three, *Trend Micro* has dropped the year from the product name, but little in *PC-cillin's* interface seems to have changed since the last *Windows 95* comparative. Detection of whole new classes of (potential) Internet-borne nasties, such as hostile Java and ActiveX applets, has been added, but for now these remain untested by *VB*, as does the Eudora Scan Mail plug-in.

PC-cillin's In the Wild detection has slipped slightly relative to the previous *Windows 95* and recent *NT* comparatives, missing some of the newly-added samples. It was one of the few products to detect both of the new macro viruses in that test-set (Header.A and Mess.A), and only the somewhat surprising miss of four Concept.W samples prevented it from registering 100% detection against the Macro test-set. Aside from the slight slip in ItW detection, *Trend's* recent efforts to catch up with the better-established names continues to show with improvements against the other test-sets.



PC-cillin is not the most dynamic of performers. It falls in that group of five products towards the bottom of the stakes, with throughput ranging around 800 KB/s on the clean hard disk test and 20 KB/s on the floppy disk test.

On-access detection was identical to the on-demand result. The Read and Write test condition is effectively *PC-cillin's* default on-access scanning configuration. However, with 50% overhead you may well be tempted to use the 'advanced' configuration options to set on-access scanning to monitor only reads or writes, reducing the overhead to a more acceptable 25%.

Conclusion

So, after reading all this, which product is best? What should you buy? And why does *Virus Bulletin* not rate products with rows of shiny blobs?

Taking up the last question first, we could have reviewed the features by reading the boxes and the reviewers' guides some products included. We could have decided that 96.6% against the Macro set was a four-blob effort and 96.7% or better a five-blob one, and so on. Fortunately, *VB* readers are *VB* readers for precisely the reasons we do not do this.

You know the average age and performance of your PCs, the management and policy guidelines you have to work to, the likely risks in your organization and the 'acceptable risk' this all adds up to. You will also be aware of the strengths and weaknesses of your current anti-virus strategy and, our results will help you to make a better informed decision on which product to use.

It is pleasing to see the regularly-tested products maintaining or slightly improving their overall detection rates, and we will follow the fortunes of the newcomers with interest in subsequent *Virus Bulletin* tests.

So, where do you start? Look at the products that had 100% detection in both In the Wild test-sets and very high Macro detection. If none of these fill your other requirements, products scoring 95% or more, consistently, across test-sets and across reviews should be worth considering. With the continual increase in virus numbers, a single test result is not as important as the vendor's long-term commitment to product development and success in maintaining the level of defence its product provides.

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 95*. These were networked to a *NetWare 3.12* server, running on a *Compaq* Prolinea 590 with 80 MB of RAM and 2 GB hard disk. 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 just one workstation and it was not connected to the network for the duration of the timed tests.

Speed and Overhead Test-sets: Clean floppy: 43 COM/EXE files, occupying 997,023 bytes on a 1.44 MB diskette. Infected floppy: The same files infected with Natas.4744, occupying 1,201,015 bytes on a 1.44 MB diskette. Clean Hard Disk: 5500 COM/EXE files, occupying 546,932,175 bytes, copied from CD-ROM to hard disk. The overhead test-set is the first 200 files from the CD-ROM, occupying 21,242,293 bytes.

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

Errata

Virus Bulletin apologizes to *IBM* and *iRiS Software*. Following a lengthy investigation, we have found some errors in the In the Wild Boot test results published in the January *Windows 95* comparative review. We reported that both products missed two samples from that test-set – Michelangelo and MISiS.

On re-testing these products on the original test machine and several others, *IBM AntiVirus* and *iRiS AntiVirus* always detected these viruses. Other products that also failed to detect these viruses in the original test still failed to detect them in the re-testing. Efforts to reproduce the conditions that led to the original testing failure have been unsuccessful. As a precautionary measure *Virus Bulletin* will not use the computer that gave rise to the suspect January results in future boot sector testing.

Unfortunately, this error means that *IBM AntiVirus for Windows 95* was not recognized with the VB 100% award it deserved. *Virus Bulletin* would like to thank the technical staff at *IBM* for their assistance in attempting to locate the source of this error. Subsequent reprints of the January test results will contain the correct scores.