COMPARATIVE REVIEW

Windows 2000 Advanced Server

Matt Ham

This has been a year for new platforms for the VB100% award, with AV products for *Linux* and *Windows XP* already having been submitted to the trials and tribulations of the test procedures. On this occasion the test platform is less novel, yet still untested in its server version: *Windows 2000 Advanced Server.*

This server product is not radically different from the venerable *Windows NT Server*, and the problems encountered with the products on test were (in most cases) overcome easily, being the same as those encountered many times before on the older platform.

Also this month, a potential long-term problem vanished from the test sets. After, by virus standards, an eternity in the In the Wild (ItW) test set, Michelangelo finally dropped out of this month's test. This was the last boot sector virus in the set to have a file system which appears corrupt to most, if not all, *Windows* installations, and for this reason was more difficult to detect for some products.

As for additions to the test set, all but four were what are these days the usual suspects, the *Windows*-executable-based worm. A notable newcomer, in type if not difficulty of detection, was BAT/Hitout.A. This is the first batch virus to be In the Wild since BAT/911, and thus potentially could have caused problems due to extension. However, these problems did not materialise in practice.

Further Clarifications

At regular intervals discussions arise as to exactly what a VB 100% award actually means. Although developers are generally aware of the exact relevance, it appears that some end-users have been examining the figures in a manner which somewhat distorts the meaning of the award. Another frequent question we are asked by readers is 'which product is best?', which falls into a related category.

A VB 100% award denotes that the product tested showed, in its default mode, 100 per cent detection of In the Wild test samples and no false positives in a selection of clean files. For on-demand scanning of files, detection is considered to be a note in the product log file that the file is infected or very likely so. For on-demand scanning of boot sector viruses, a notification or log file entry is required.

For on-access scanning the matter is a little more confusing, since the best method of testing – executing all files and using the results from this activity – is clearly impractical.

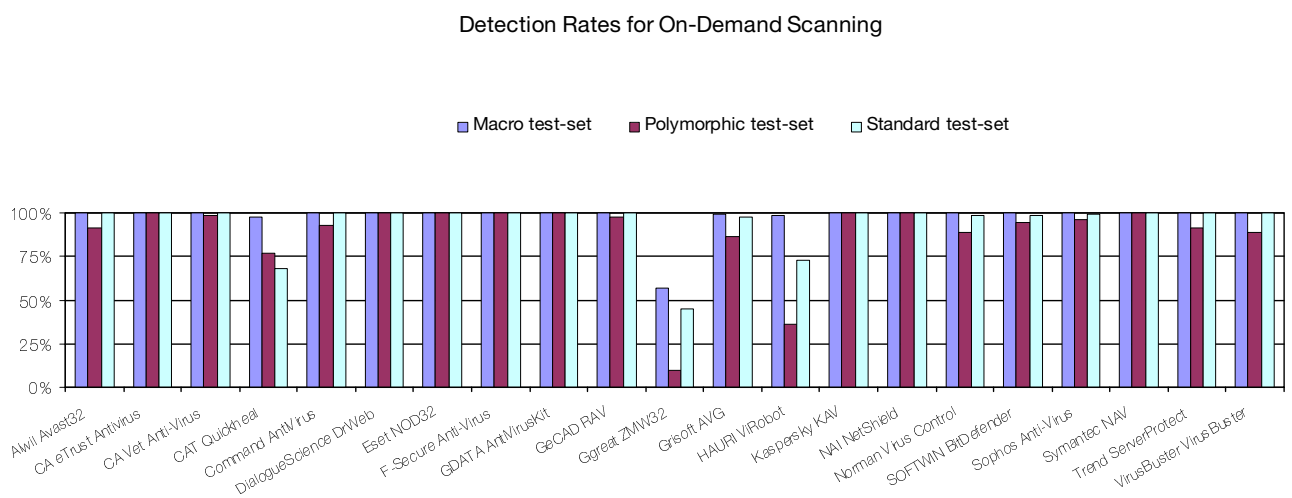
On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast32	0	100.00%	0	100.00%	100.00%	14	99.66%	144	91.13%	13	99.73%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	0	100.00%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	436	98.58%	4	99.78%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	110	97.25%	3774	76.85%	613	67.68%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	133	93.02%	12	99.61%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.85%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	35	97.61%	2	99.88%
Ggreat ZMW32	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Grisoft AVG	2	99.58%	0	100.00%	99.60%	20	99.51%	251	86.05%	59	97.65%
HAURI ViRobot	1	99.83%	0	100.00%	99.84%	69	98.19%	10695	35.96%	N/A	N/A
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI NetShield	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	7	99.49%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	650	88.92%	31	98.58%
SOFTWIN BitDefender	0	100.00%	11	0.00%	94.74%	0	100.00%	126	94.73%	2	99.88%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	11	99.73%	60	95.79%	18	99.42%
Symantec NAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	13	99.87%
Trend ServerProtect	9	98.94%	0	100.00%	99.00%	0	100.00%	292	91.15%	8	99.82%
VirusBuster VirusBuster	0	100.00%	8	27.27%	96.17%	49	98.96%	160	89.13%	11	99.67%

Detection is thus judged by a product denying access to an infected file when the file is opened for writing.

For boot sector on-access scanning a visible notification or log file entry is required. In this case denial of access is not a useful guide to detection since the *VB* boot sector test floppies are all blank as far as file contents are concerned. Since denial of access is likely to show a blank disk as the only detectable effect, this is not particularly useful. The addition of extra files to the disk for use in deciding whether access has been denied was decided against, for in past testing some products were only able to detect a boot sector virus on a floppy containing other files – a situation which would be apparent only with the use of disks in their current state.

There have been products which, by design, do not scan on access except on file execution. Thankfully, those that are designed this way becoming fewer overall. More problematic are those products which cannot be cajoled into producing reasonable logs on demand, thus making detection checking problematic. These are checked by setting the product to delete and/or disinfect. The files are then scanned until no more detections are present, if necessary manually noting those files which are detected as infected but are not deleted or disinfected. Disinfected files are removed from the test set by use of CRC checking, and those files left in the test set are considered to be misses.

This said, there remains ample opportunity for products to miss detection, in our tests, of files which they are perfectly



able to detect – which begs the question, why should this be so? The answers are potentially many, though two are more relevant than others. First, there are the matters of default extension lists, a common area for failure over the years. In particular *Kaspersky Anti-Virus* and *NAI* products have failed to gain a number of VB 100% awards because the default extension lists did not include possible extensions for In the Wild viruses. In most cases these extension-based problems are easily solved by an administrator adding extensions to the default list. We could perform these changes prior to testing. We feel, however, that our readers are better served if they know that they have to do this, than if we scan all files regardless of extension.

Another example of why some products miss out on VB 100% awards, is where certain files are not scanned directly on-access. The usual assumption by the product developers is that the files will be scanned when passed on to an application which makes use of them. At the most common level this covers such objects as ZIP files, which are often not scanned until unzipped. In some past tests *Aladdin*'s products fell into this category where OLE files were concerned, scanning these only when passed to, for example, *Word*. The most recent example of this behaviour has been the *FRISK* treatment of EML files, which are not scanned until individual mails are pulled from within (see this issue, p.3). From a developer's point of view these choices make sense in that leaving objects unscanned until use creates fewer overheads. The chance of infection on a protected machine is not increased, since scanning will occur before code execution.

Such treatment of objects does, however lead to misses under the VB 100% testing methodology, which brings us back to the original questions. In short, the answers are as follows. A VB 100% award means that a product has passed our tests, no more and no less. The failure to attain a VB 100% award is not a declaration that a product cannot provide adequate protection in the real world if administered by a professional. As to which product is 'best', this all depends on the interaction between the anti-virus software, installed hardware and software and that same administrator. We would urge any potential customer, when looking at the VB 100% record of any software, not simply to consider passes and fails, but to read the small print in these reviews.

Alwil Avast32 3.0.499.2

ItW Overall	100.00%	Macro	99.66%
ItW Overall (o/a)	100.00%	Standard	99.73%
ItW File	100.00%	Polymorphic	91.13%

As ever, misses in detection were scattered through the non-ItW sets with a definite favouring of the polymorphic set for non-detection. The *Alwil* interface is one of the more complex and customisable of those on offer, though it seemed that on-access scanning had become simpler to configure. This might have been as a result of finding a control already in existence, though unseen before. Whatever the reasons, the testing ran smoothly. With no false positives and full detection In the Wild, Avast 32 chalks up the first VB 100% of this review.

Cat Computer Services QuickHeal X Gen 6.05

ItW Overall	100.00%	Macro	97.25%
ItW Overall (o/a)	100.00%	Standard	67.68%
ItW File	100.00%	Polymorphic	76.85%

Another relative newcomer to the comparative scene, *Quickheal* showed improvements in detection. From a historic-virus viewpoint detection remains weak in some areas, though as more modern threats are considered the detection rate improves rapidly. Speed of scanning is good too, which leaves only the matter of false positives as a possible fly in the ointment. Again this is an area where rapid improvements have occurred, and a lack of false positives and a full detection of In the Wild Viruses gains *QuickHeal* a VB 100% award.

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil Avast32	0	100.00%	0	100.00%	100.00%	14	99.66%	144	91.13%	13	99.73%
CA eTrust Antivirus	0	100.00%	0	100.00%	100.00%	4	99.90%	0	100.00%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	436	98.58%	2	99.90%
CAT Quickheal	0	100.00%	0	100.00%	100.00%	110	97.25%	3774	76.85%	613	67.68%
Command AntiVirus	0	100.00%	0	100.00%	100.00%	0	100.00%	133	93.02%	10	99.73%
DialogueScience DrWeb	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	1	99.98%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
F-Secure Anti-Virus	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	1	99.98%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
GeCAD RAV	0	100.00%	0	100.00%	100.00%	0	100.00%	35	97.61%	2	99.88%
Ggreat ZMW32	274	54.80%	0	100.00%	57.18%	1805	56.46%	14772	9.84%	1056	45.08%
Grisoft AVG	2	99.58%	0	100.00%	99.60%	20	99.51%	251	86.05%	59	97.65%
HAURI ViRobot	1	99.83%	0	100.00%	99.84%	69	98.19%	10695	35.96%	541	72.80%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
NAI NetShield	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	4	99.63%
Norman Virus Control	0	100.00%	0	100.00%	100.00%	0	100.00%	650	88.92%	29	98.71%
SOFTWIN BitDefender	1	99.92%	0	100.00%	99.92%	14	99.64%	121	94.76%	47	98.30%
Sophos Anti-Virus	0	100.00%	0	100.00%	100.00%	8	99.80%	60	95.79%	18	99.42%
Symantec NAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	13	99.87%
Trend ServerProtect	9	98.94%	0	100.00%	99.00%	0	100.00%	292	91.15%	8	99.82%
VirusBuster VirusBuster	0	100.00%	0	100.00%	100.00%	0	100.00%	160	89.13%	8	99.82%

Command AntiVirus for Windows 4.73.1

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.73%
ItW File	100.00%	Polymorphic	93.02%

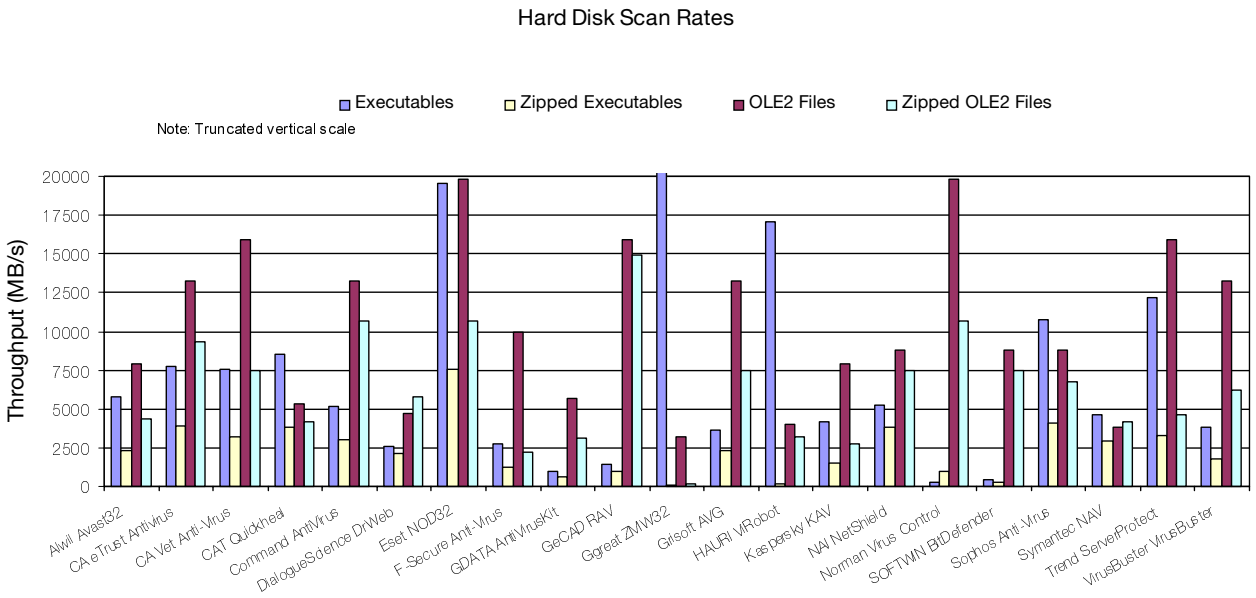
Historically, *Command AntiVirus* has been a pleasure to review, with easy installation, operation and log file analysis. Now, however, log files are by default, produced in RTF format – which rendered useless the standard file comparison tools used in log analysis. The hidden RTF content more than doubled the size of the report file as compared with a plain text version of the same data. These irritations aside, *Command AntiVirus* earned a VB 100%.

Misses were mostly among the modern W32 polymorphics, notably W32/Fosforo, W32/Etap, W32/Tuareg.B and W32/Zmist.D. There were also some small floppy change detection problems when testing these on access.

Computer Associates eTrust Antivirus 6.0.96 23.57.56

ItW Overall	100.00%	Macro	99.90%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

As is becoming traditional for *eTrust*, a selection of mandatory patches needed to be applied on installation.



However, these were more automated than I remember. Not quite so good is the slightly confusing labelling of updates on the *CA* site. Also, the update instructions fail to note that manual halting of services within *eTrust* is required before patching can occur. After installation, however, results were of the customary high standard. Even the commonly missed samples of W32/Etap were detected, though samples of W97M/Box.A were missed. Fortunately these were no barrier to *eTrust Antivirus* earning a VB 100%. With reference to the comments made earlier in this review, W32/Heidi.A samples embedded within zip files were detected on demand, though not on access.

Computer Associates Vet Anti-Virus 10.52.02

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.90%
ItW File	100.00%	Polymorphic	98.58%

Vet is less burdened or blessed (depending upon user needs) with integration into other *Computer Associates* products than *eTrust Antivirus*, which adds to its simplicity of use in this kind of test. The age-old cry of weakest in the polymorphics goes up yet again – with detection elsewhere being all but perfect. Remaining quite speedy on scanning, and with no false positives, *Vet* earns *Computer Associates* another VB 100% award.

DialogueScience DrWeb for Windows 95-XP 4.28c

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.98%
ItW File	100.00%	Polymorphic	100.00%

DrWeb has had a history of good results in *VB* comparative testing, which has also accompanied a gradual improvement in interface clarity for the on-access component. The number of suspicious files on this occasion was only one. All but one detected sample in the test set were detected exactly without recourse to heuristic methods, leaving only ZIP-encoded W32/Heidi.A files on access and the TMP sample of W32/Nimda.A as misses. Since the latter is included only as a curiosity in the standard set, *DrWeb* gains another VB 100% award.

Eset NOD32 1.314

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItWmFile	100.00%	Polymorphic	100.00%

NOD32 remained speedy, but was rivalled on this occasion by other products. As far as detection was concerned, full In the Wild detection for both boot and file viruses was sufficient to garner another VB 100% award for the product. Misses were, in fact, absent in any test set.

F-Secure Anti-Virus 5.40

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.98%
ItW File	100.00%	Polymorphic	100.00%

Sporting a combination of two engines, neither of which are poor at detection, it comes as no surprise that *FSAV* collects another VB 100% award. As is a common theme in this review, the ZIP files containing W32/Heidi.A were the only misses of any note.

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (MB/s)	FPs [susp]	Time(s)	Throughput (MB/s)	FPs [susp]	Time (s)	Throughput (MB/s)	Time(s)	Throughput (MB/s)
Alwil Avast32	94	5818.4		10	7933.4		69	2310.4	17	4388.7
CA eTrust Antivirus	71	7703.3		6	13222.3		41	3888.2	8	9325.9
CA Vet Anti-Virus	72	7596.3		5	15866.8		50	3188.3	10	7460.7
CAT Quickheal	64	8545.8		15	5288.9		42	3795.6	18	4144.9
Command AntiVirus	107	5111.5		6	13222.3		52	3065.7	7	10658.2
DialogueScience DrWeb	214	2555.8	[1]	17	4666.7		75	2125.6	13	5739.0
Eset NOD32	28	19533.3		4	19833.4		21	7591.3	7	10658.2
F-Secure Anti-Virus	201	2721.1		8	9916.7		130	1226.3	33	2260.8
GDATA AntiVirusKit	585	934.9	1	14	5666.7		244	653.3	24	3108.6
GeCAD RAV	377	1450.7		5	15866.8		166	960.3	5	14921.5
Ggreat ZMW32	18	30385.1	4	25	3173.4		2068	77.1	413	180.6
Grisoft AVG	150	3646.2	[5]	6	13222.3		70	2277.4	10	7460.7
HAURI ViRobot	32	17091.6	[1]	20	3966.7		928	171.8	23	3243.8
Kaspersky KAV	132	4143.4		10	7933.4		104	1532.9	27	2763.2
NAI NetShield	104	5259.0		9	8814.9		42	3795.6	10	7460.7
Norman Virus Control	1792	305.2		4	19833.4		167	954.6	7	10658.2
SOFTWIN BitDefender	1156	473.1	1	9	8814.9		549	290.4	10	7460.7
Sophos Anti-Virus	51	10724.2		9	8814.9		39	4087.6	11	6782.5
Symantec NAV	118	4635.0		21	3777.8		55	2898.5	18	4144.9
Trend ServerProtect	45	12154.0		5	15866.8		49	3253.4	16	4663.0
VirusBuster VirusBuster	142	3851.6		6	13222.3		88	1811.6	12	6217.3

GData AntiVirusKit Professional 11.0.4

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

The second multiple-scan-engine product in this review and again the policy seems to have paid off. In *GData*'s case the result is a total absence of missed files in any test set. However, a false positive for *AVK* can be blamed for its failure to carry off the VB 100% award on this occasion.

GeCAD RAV AntiVirus Desktop 8.6.103

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.88%
ItW File	100.00%	Polymorphic	97.61%

Like many of the other products this month, *RAV* passed through the review process without hiccups. W32/Heidi in its ZIP archive was missed both on access and on demand, together with W32/Etap, one sample of W32/Fosforo and some more surprising samples of Cryptor. None of these were In the Wild, however, and *RAV* gains a VB 100% award.

Ggreat ZMW32 virus scan M7.5+

ItW Overall	57.18%	Macro	56.46%
ItW Overall (o/a)	N/A	Standard	45.08%
ItW File	54.80%	Polymorphic	9.84%

Ggreat's product is new to the *VB* comparative tests, and enters at a slight disadvantage by nature of its design. Primarily, it is a scanner for incoming emails, and as such,

has no other on-access portion. This disqualifies it from a VB 100% award. As far as detection overall was concerned, selection of directories seemed to have unpredictable results as to how many were scanned, so the scanning was performed in areas rather than the whole collection in one batch. Stability problems were encountered when repair was selected.

GriSoft AVG 6.0 build 398

ItW Overall	99.60%	Macro	99.51%
ItW Overall (o/a)	99.60%	Standard	97.65%
ItW File	99.58%	Polymorphic	86.05%

AVG brought a slight need for the use of judgement to the definition of default mode, since it offers three scan types as existing options from its main scan interface. Of Quick, Complete and Main, Main was selected as the default scan type on the basis of its name.

HAURI ViRobot 4.0

ItW Overall	99.84%	Macro	98.19%
ItW Overall (o/a)	99.84%	Standard	72.80%
ItW File	99.83%	Polymorphic	35.96%

ViRobot has been one of the recent marked improvers in performance in VB 100% testing, and this review showed increased detection again. The log files available in the product are, however, still limited in size to such an extent that they are not useful for testing purposes. Detection was judged here by deletion of some infected files and disinfection of others, followed by deletion of those files with an altered CRC. Of note in this process was W32/Beast which, in its DOC samples, was flagged as being removable only upon the next boot.

A rather larger problem was encountered when the standard set was scanned on access. On several samples in this set the machine would reproducibly blue-screen with an error which looks likely to be related to unpleasant pitfalls within these samples. The Standard test set was eventually listed as untested on access due to time constraints.

Kaspersky Anti-Virus 4.0.5.35

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	100.00%

Kaspersky Anti-Virus was for a long period a scanner that could do no wrong in *VB* comparatives, though suffering from a hiatus mainly brought about by extension issues. These issues seem to have been dealt a serious and happy fatal blow. Misses in the test set were completely absent, as were false positives. *Kaspersky Anti-Virus* earns another VB 100% award.

NAI NetShield 4.5 4.1.60 4.0.4227

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.63%
ItW File	100.00%	Polymorphic	100.00%

Another a product which has suffered from issues with extensions in its recent history, and another which seems to have overcome these lately. Although the optional all-file scanning patch was not applied, its status being definitely not a patch which is required to keep the product up to date, this did not harm the results in any way. Misses were confined to the common W32/Heidi on-access and to this Cruncher was added – another virus which encodes itself, in this case using DIET. *NetShield* produced no false positives and thus a VB 100% award is awarded.

Norman Virus Control 5.4

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	98.71%
ItW File	100.00%	Polymorphic	88.92%

Norman remains unique in its method of scan job construction, a feature which has ceased to be a novelty when reviewing. One major change that has occurred is that the product once again produces log files without recourse to undocumented features.

The slowdown on the *VB* clean executable test remains all the more strange because it is not reflected when the same files are scanned in zipped format. Weakest on polymorphics but with a clean record on false positives, *NVC* gains a VB 100% award for *Norman*.

SOFTWIN BitDefender Professional 6.4.3

ItW Overall	99.92%	Macro	96.64%
ItW Overall (o/a)	94.74%	Standard	98.30%
ItW File	99.92%	Polymorphic	94.76%

BitDefender continues to show reasonable detection rates in all sets, though missing out on some scattered samples, most notably amongst the polymorphics. A single miss of the HTM sample of W32/Nimda.A In the Wild, however, was sufficient to deny the product a VB 100% award. This was most likely due to choices in the implementation of on-demand scanning, since the same file was detected on access.

Matters were more clear cut when it came to problems in the on-access boot sector testing. During these tests no alerts were triggered at any time. Similarly, no detection was logged by the various statistical methods on offer for examining scan results, and this test set thus drew an effective blank as far as detection was concerned.

Sophos Anti-Virus 3.62

ItW Overall	100.00%	Macro	99.80%
ItW Overall (o/a)	100.00%	Standard	99.42%
ItW File	100.00%	Polymorphic	95.79%

The *Sophos* product showed a significant cosmetic change, with a whole new corporate image having been impressed upon it. However, the product itself and the majority of the GUI remains the same.

With only superficial changes to the product, scanning matters changed little if at all. Those files missed were those missed by *SAV* since time immemorial (Positron, Navrhar and the like), in addition to a fair number of the newer polymorphic viruses. Since none of these are from the ItW set, *SAV* earns itself another VB 100% award.

Symantec Norton AntiVirus Corporate Edition 8.00.9374

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.87%
ItW File	100.00%	Polymorphic	100.00%

Norton AntiVirus showed its usual good rates of detection, though not without some oddities creeping in. BAT/911.A was missed both on access and on demand, and perhaps more oddly, W97M/Antisocial.F was apparently missed only on demand – a virus having previously had perfect detection. This turned out to be due to an odd quirk in logging for this virus which declared non-existent files to be infected, while making no mention of the existing files. Despite this odd behaviour, which was noted as a detection nonetheless, and slow scanning of infected sets, results were otherwise excellent and *NAV* gains another VB 100% award for its pains.

Trend ServerProtect 5.35 1047

ItW Overall	99.00%	Macro	100.00%
ItW Overall (o/a)	99.00%	Standard	99.82%
ItW File	98.94%	Polymorphic	91.15%

Trend's offering suffered from slightly dated virus definitions. A definition update was promised, but did not arrive. Given that the misses that occurred in this test included W32/Surnova.D and W32/Datom.A, recent additions to the In the Wild set, it is likely that this lack of upgrade had an effect upon detection rates. Blame for the lack of a VB 100% award, however, cannot be laid entirely at the foot of this update issue, since an ItW sample of W32/CTX.A was also missed. Other than this, detection was very good except in the polymorphic sets, traditionally a weak spot, and the category under which W32/CTX.A can also be placed.

VirusBuster for Windows 3.10

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	96.17%	Standard	99.82%
ItW File	100.00%	Polymorphic	89.13%

VirusBuster's initial installation resulted in a blue screen upon the required reboot after installation. However, the reference to a bad pool caller was not reproducible either on this initial installation or on a second installation on a fresh image of the operating system. The latter installation was used for testing, in case the initial blue-screen had left *VirusBuster* in some way defective.

Problems were apparent in the on-access scanning of boot sectors, where change detection was in a league of its own as far as irritation was concerned. In several sessions of testing, and two further reinstallations, three viruses were detected once on access, after which detection seemed not to exist. Given the good results on other scanning, this comes as something of a disappointment.

Other than these on-access woes there was full detection of all but a scattering of polymorphic samples, with no false positives. A close approach to a VB 100% award, scuppered by boot sectors.

Conclusion

The most notable feature of this review, from a practical point of view, was the contrast with the recent *Windows XP* comparative. In that review the problems encountered both on installation and operation were many. In this review the problems were few, far between and by and large reserved for those products less frequently reviewed. This can be ascribed to the additional age of *Windows 2000 Advanced Server* and to its similarity to *Windows NT Server* – both of which factors will have given developers ample time to iron out any odd bugs.

This difference in performance goes a long way towards explaining why many businesses seem to lag far behind the times when it comes to upgrading operating systems. *Windows NT* and *2000* still hold sway in great swathes of the corporate market, and the stability of time-tested software upon them plays a large part in this reluctance to speed on to the newest platform of *XP*. It is not without reason that some users prefer platforms that the manufacturers now decry as being feature-barren, antiquated and due for replacement.

Technical Details

Test environment: Three 1.6 GHz Intel Pentium 4 workstations with 512 MB RAM, 20 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy, all running *Windows 2000 Advanced Server Service Pack 2*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win2K/2002/test_sets.html.

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

Addendum: *Windows 2000 Advanced Server* Comparative Review

In the November 2002 Comparative Review *Trend's ServerProtect* was reported to have failed to achieve full detection of ItW virus samples and thus was not given a VB 100% award (see *VB* November 2002, p.23). The review stated, '*Trend*'s offering suffered from slightly dated virus definitions. A definition update was promised, but did not arrive.' Following further investigation, however, it has come to light that fate conspired against the developers at *Trend* who sent the update at the exact time that *VB* was suffering a mail server outage. Mail servers rectified, the updates were re-sent, installed, tested and we are happy to announce that *Trend ServerProtect 5.35 1047* earned a VB 100% award, having detected all samples in the ItW set – including W32/CTX.A – and generated no false positives. We apologise to *Trend* for the problems ∎