

COMPARATIVE REVIEW

WINDOWS 2003 SERVER

Matt Ham

Another comparative review and another new operating system enters the VB labs to be overloaded and treated far worse than perhaps it deserves. New OSs are always good for revealing bizarre new faults in previously unbreakable pieces of anti-virus software. The areas in which novelty has previously caused difficulties have been with the on-access scanners, and in particular, floppy disk scanning on access. Having experienced red faces in the past, I imagined developers would have become somewhat more careful on these matters, though some slip-ups were expected to unfold as the review progressed.

Windows 2003 Server itself was relatively pleasant to work with. One feature I found intriguing was that, under *Windows 2003 Server*, anti-virus products are expected to be able to run simultaneously. Various developers have mentioned this feature as having worked to a greater or lesser extent in their ad hoc tests – which is a mixed blessing. If 95 per cent of two product combinations work simultaneously (which is what most results seem to indicate), this may encourage people to run two on-access scanners on mission-critical machines. This may delight the 95 per cent, but there will be gnashing of teeth for those who discover themselves amongst the incompatible 5 per cent. This feature did inspire some crazy thoughts of using just one test machine to perform all the comparative tests simultaneously – though this is perhaps something I shall suggest other reviewers do, while sniggering quietly to myself.

Although the deadline for product submissions for this test was 6 October, the test sets were based upon the July 2003 WildList – a long delay indeed. However, this was the newest data available at the time (blame for which may partially be laid at the door of the *Virus Bulletin* conference for having dragged the WildList team away from their desks). Although new WildList data was available three days after the deadline, this data was not used as it was from the newly inaugurated Real-Time WildList. In future reviews VB plans to use WildList data from approximately 24 hours before the comparative deadline. There are still some issues to be decided, since this will make geography a real factor in the submission of products – but expect more potential for failure in the months ahead.

As for additions to the test sets this month, there were rather more than the usual bunch and a selection across the various types. Most unusually, a batch virus, BAT/Mumu.A, made its way into the wild, as well as the slightly more common sprinkling of macro viruses. Of particular note when replicating these new samples were the number now

attempting to use peer to peer networks as a form of propagation. This feature leads to huge numbers of supposedly tempting-sounding files lurking in folders. While I admit that some individuals might be tempted by Jennifer Lopez engaged in amorous pursuits with a lavatory, one would hope that a user seeking complete guides to PHP4 might realise that these are unlikely to be distributed as .EXE files via *Kazaa*. Such diversions aside, the test sets looked to contain few horrors for the products and a bumper crop of VB 100% awards was anticipated.

AhnLab V3Net SE SP2

ItW Overall	100.00%	Macro	98.18%
ItW Overall (o/a)	100.00%	Standard	85.42%
ItW File	100.00%	Polymorphic	45.48%

While *V3Net*'s pastel colour scheme looked somewhat out of place on the staid desktop of *Windows 2003*, its performance did not suffer. Misses were slightly higher on access than on demand, but there were no misses in the wild. However, the treatment of infected items was rather bizarre. In most cases objects are deleted or disinfected through the use of a dialog box which pops up. I was unable to predict quite when this box would pop up and there were similar arbitrary delays in infection reports reaching the log file. As a general rule, the older the virus, the less chance there is of *V3Net* detecting it. Thus, while detection of older macro, standard and polymorphic viruses was relatively poor, newer threats were well detected. This selective detection pays dividends elsewhere, with very fast scanning rates and a zero false positive rate – which adds up to a VB 100% award for *AhnLab*.



Alwil Avast! 4.1.29

ItW Overall	99.58%	Macro	99.56%
ItW Overall (o/a)	N/A	Standard	99.73%
ItW File	99.56%	Polymorphic	91.21%

Avast! was the most obvious victim of the move to a new OS, with mysterious service failures appearing after installation. The program also declared that the virus vault and resident protection job were being supplied with null initialisation data and thus failed to operate. This made the on-access portion of the program impossible to test. In addition to these problems there was another reason for the product missing out on a VB 100%, with BAT/Mumu.A being missed in the ItW set. However, detection was otherwise good and the product continues to be enhanced with each release. It was a moment of joy indeed when I

On-access tests	ItW File		ItW Boot		ItW Overall		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	0	100.00%	0	100.00%	0	100.00%	81	98.11%	9239	42.74%	314	85.38%
Alwil Avast!	-	-	-	-	-	-	-	-	-	-	-	-
CA eTrust Antivirus	0	100.00%	0	100.00%	0	100.00%	4	99.90%	1	99.89%	2	99.88%
CA Vet Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	99.87%	4	99.78%
CAT QuickHeal	0	100.00%	0	100.00%	0	100.00%	107	97.45%	1086	92.85%	660	60.88%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	97.53%	3	99.79%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	3	99.85%
GDATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	0	100.00%	23	99.44%	925	81.40%	47	97.15%
Kaspersky KAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	11	99.69%
MicroWorld eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	11	99.69%
NAI McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	3	99.67%	0	100.00%	0	99.68%	-	-	-	-	-	-
NWI VirusChaser	1	99.56%	0	100.00%	1	99.58%	4	99.90%	0	100.00%	4	99.69%
SOFTWIN BitDefender	0	100.00%	0	100.00%	0	100.00%	13	99.69%	22	96.55%	40	98.88%
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	8	99.80%	18	98.06%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend ServerProtect	0	100.00%	0	100.00%	0	100.00%	0	100.00%	215	95.77%	1	99.98%
VirusBuster VirusBuster	0	100.00%	0	100.00%	0	100.00%	0	100.00%	101	91.45%	11	99.67%

realised that the extremely long registration keys have been replaced by a registration file. Sadly, however, constant improvements are likely to be the cause of the new problems.

CA eTrust Antivirus 7.0.139

ItW Overall 100.00% **Macro** 99.90%
ItW Overall (o/a) 100.00% **Standard** 100.00%
ItW File 100.00% **Polymorphic** 99.89%

Having stumbled somewhat in the last comparative review, *eTrust Antivirus* returned to its customary excellent

detection rates this month. The patching process has always been a part of *eTrust's* installation, and in this case three patches and two updates were required for installation. However, the patching process was rather more automated than previously, which made this task much less arduous. Unfortunately, not all change is good, and this was most obvious in the logging features of *eTrust*. These are now entirely binary while stored, with the exported versions being formatted in such a way as to render them all but useless. Only the very small number of missed samples made it feasible to use the logs at all – by selecting the toggles for displaying misses only, and reading the results from the screen. More disturbing than this, however, was the

sudden arrival of false positives in the clean set, which denied *eTrust* a VB 100%.

CA Vet Anti-Virus 10.59.2

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.90%
ItW File	100.00%	Polymorphic	99.87%

Matters looked hopeful for *Vet*, as it was the only product of those reviewed to declare itself loudly as being a specifically *Windows 2003* product. *Vet*'s detection rate for polymorphics was vastly improved over past results. This does not seem to have added any huge slowdown for the clean set timings and neither were any false positives noted. The improved detection rate included a full detection in the ItW test set, thus earning *Vet* a VB 100% award.



CAT QuickHeal X Gen 7.0

ItW Overall	100.00%	Macro	97.54%
ItW Overall (o/a)	100.00%	Standard	82.60%
ItW File	100.00%	Polymorphic	92.89%

QuickHeal is another product opting for the non-detection of a variety of older viruses. Of particular note is the much higher detection rate in the standard test set when on-demand rather than on-access scanning is performed. The same trend is seen in the standard and macro virus sets, though not to the same extent. This does make some logical sense in that the undetected viruses in question are very unlikely to be able to operate on a modern machine. Full detection of ItW viruses, coupled with a distinct lack of false positives, means that a VB 100% is awarded to *QuickHeal*.



DialogueScience Dr.Web 4.30

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

Dr.Web achieved full detection over all the test sets and consequently earns a VB 100% award. Of note was a new feature that had crept into the *Dr.Web* installation routine. What I took at first to be a very short licence affirmation was in fact a declaration that no other anti-virus program was running on the machine. Without this the installation would not proceed. Though this should be an unnecessary precaution on



Windows 2003 it is certainly a useful method of encouraging users to be more careful when installing products. Also of note was the flagging of suspicious files. Only one file was flagged as suspicious, but when scanning the same files in zipped form the number of suspicious files increased dramatically. This is not surprising given the predilection of viruses to use multiple encryption and packing methods – clearly there are heuristic methods at work with that premise.

Eset NOD32 1.529

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

NOD32 produced an unsurprising 100 per cent detection rate and thus earns a VB 100% award. There was one fly in the ointment which affected many of the products in this review – this is by no means specific to *NOD32*, and neither was *NOD32* one of the worst offenders. The problem is that over 50 per cent of the products require a reboot when installing. Given that *Windows 2003 Server* is a server platform, this seems likely to irritate administrators no end. Most distressingly, three of the products on offer (*Vet*, *Dr.Web* and *VirusChaser*) required reboots when changing on-access configuration. This is frustrating enough when testing the products, but would be far more so on, for example, a company's main SQL server.



FRISK F-Prot Antivirus 3.14b

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.79%
ItW File	100.00%	Polymorphic	97.53%

F-Prot AntiVirus showed impressive detection and a lack of false positives. This was amply sufficient to be rewarded with a VB 100% award. It is worth mentioning here that *FRISK*'s *Linux* product will be undergoing a standalone review in the next issue. In the last *Linux* Comparative the on-access component proved intractable on our test machines and we hope to do the product more justice upon this occasion.



F-Secure Anti-Virus for Servers 5.41

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.98%
ItW File	100.00%	Polymorphic	99.92%

On-demand tests	ItW File		ItW Boot		ItW Overall		Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%	Number missed	%
AhnLab V3Net	0	100.00%	0	100.00%	0	100.00%	79	98.18%	9119	45.48%	313	85.42%
Alwil Avast!	1	99.56%	0	100.00%	1	99.58%	18	99.56%	153	91.21%	13	99.73%
CA eTrust Antivirus	0	100.00%	0	100.00%	0	100.00%	4	99.90%	1	99.89%	0	100.00%
CA Vet Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	2	99.87%	2	99.90%
CAT QuickHeal	0	100.00%	0	100.00%	0	100.00%	101	97.54%	1078	92.89%	318	82.60%
DialogueScience Dr.Web	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Eset NOD32	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
FRISK F-Prot Antivirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	97.53%	3	99.79%
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	1	99.98%
GDATA AntiVirusKit	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	0	100.00%	20	99.51%	257	85.97%	23	99.01%
Kaspersky KAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	0	100.00%
MicroWorld eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.92%	0	100.00%
NAI McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	99.79%
Norman Virus Control	3	99.67%	0	100.00%	3	99.68%	3	99.93%	180	91.24%	4	99.87%
NWI VirusChaser	1	99.56%	0	100.00%	1	99.58%	4	99.90%	0	100.00%	0	100.00%
SOFTWIN BitDefender	0	100.00%	0	100.00%	0	100.00%	13	99.69%	23	96.50%	38	99.01%
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	8	99.80%	18	98.06%	14	99.49%
Symantec SAV	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%
Trend ServerProtect	0	100.00%	0	100.00%	0	100.00%	0	100.00%	515	94.38%	3	99.85%
VirusBuster VirusBuster	0	100.00%	0	100.00%	0	100.00%	0	100.00%	101	91.45%	8	99.82%

Without a review offer or interesting piece of gossip to fall back on, it would have helped if *F-Secure Anti-Virus* were to contain some glaring fault or bizarre easter-egg. Sadly for me this was not to be the case – the most that could be commented upon being a very slight slow down of the test machines after processing some rather vast log files. This persisted rather longer than might be expected but went away of its own accord.

After that earth-shattering revelation it will be no surprise that *FSAV* is a recipient of a VB 100% award for excellent detection and no false positives.



GDATA AntiVirusKit 12.0.5

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.92%

AVK also showed excellent detection rates. However, the *GDATA* product managed to fall at the last hurdle – by throwing up a single false positive. The fact that this was produced by the *RAV* engine adds a little poignancy to proceedings. Not only does it show that the engine, although whisked away to Redmond, is still in use

commercially, but it also allows conspiracy theorists to blame *Microsoft* for *AVK*'s failure to gain a VB 100%.

Grisoft AVG Anti-Virus System 6.0.524 321

ItW Overall	100.00%	Macro	99.51%
ItW Overall (o/a)	100.00%	Standard	99.01%
ItW File	100.00%	Polymorphic	85.97%

The *AVG* product as supplied consists of a base package upon which updates are applied as a proprietary .BIN format. Rather oddly, however, some of the updates would operate only by being selected for use manually, while others were usable by insertion into the upgrades directory of the *AVG* installation. Also somewhat mysterious was the difference in detection between on-access and on-demand scans. It is possible that this was related to time-outs during on-access scanning of complex polymorphic samples, though that is not wholly convincing. What is certain, however, is that *AVG* gains a VB 100% award, with no false positives and full detection of ItW viruses both on access and on demand.



Kaspersky KAV 4.5.0.58

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.92%

Installing a *Kaspersky AntiVirus* instance for the first time is something of a long-winded chore since numerous definition files must be layered one upon another before the product can be used. After installation the update process is rather easy and automated. As might be expected by this stage *KAV* detected well – the only misses being one of W32/Etap and the .VXD samples of Navrhar on-access, which were presumably avoided for reasons of scanning speed. Less predictable was the behaviour of on-access floppy scanning. Detection of disk changes was extremely variable and the only rational explanation for the times at which scanning occurred seemed to be that the on-access scanning was on a mini-schedule, ignoring disk changes and simply scanning at intervals. However, with no problems concerning detection or false positives, *KAV* earns a VB 100% award.



MicroWorld Software eScan 10,1,0,2

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	100.00%
ItW File	100.00%	Polymorphic	99.92%

eScan opened with an impressive display of raw confusion – a server product which declared it could not be operated ... on servers. The software was unusable as a result of a Flash animation of, among other things, an exploding planet, rendering the program no more than a rather large cartoon clip. Sadly matters became more mundane after this, and the program was able to be installed by means of ripping temporary installation files from their resting places. Full detection of all but one polymorphic file, and no false positives, led to a VB 100% award. A disappointment to me, since I was at least expecting to be assaulted by a horde of killer gannets.



NAI McAfee VirusScan 7.10 4.2.60 4296

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.79%
ItW File	100.00%	Polymorphic	100.00%

The testing of *McAfee VirusScan* did not bring back memories of the great floppy scandals of days gone by, and detection was impressive by any standards. I cannot remember a time when *VirusScan* produced a false positive in VB testing, and this review was no different. Another VB 100% is duly awarded.



Norman Virus Control 5.60.13

ItW Overall	99.68%	Macro	99.93%
ItW Overall (o/a)	99.68%	Standard	99.87%
ItW File	99.67%	Polymorphic	91.24%

To *Norman*'s chagrin the gremlins within the Sandbox technology at the heart of *NVC*'s heuristic capabilities have not yet sated their lust for fame. A false positive in the clean test set was accompanied by a warning of infection by Sandbox: W32/FileInfector. This will be irksome indeed for *Norman* but worse was to come. The on-access component of the program was highly unstable, tending to lock up the machine after being bombarded with a thousand or so viruses in short order. This problem made it impossible to perform testing in any but the ItW set, the other areas being too prone to cause the machine to enter a state of comatose narcissism. As if these woes were not enough to contend with, W95/Tenrobot.B was not fully detected in the wild.

NWI VirusChaser 5.0

ItW Overall	99.58%	Macro	99.90%
ItW Overall (o/a)	99.58%	Standard	100.00%
ItW File	99.56%	Polymorphic	100.00%

Hard Disk Scan Rate	Executables			OLE Files			Zipped Executables		Zipped OLE Files	
	Time (s)	Throughput (KB/s)	FPs [susp]	Time(s)	Throughput (KB/s)	FPs [susp]	Time (s)	Throughput (KB/s)	Time(s)	Throughput (KB/s)
AhnLab V3Net	23	23779.7		8	9916.7		46	3465.6	15	4973.8
Alwil Avast!	168	3255.5		16	4958.4		117	1362.5	30	2486.9
CA eTrust Antivirus	87	6286.6	2	4	19833.4		52	3065.7	8	9325.9
CA Vet Anti-Virus	78	7012.0		7	11333.4		49	3253.4	10	7460.7
CAT QuickHeal	60	9115.5		11	7212.2		45	3542.6	16	4663.0
DialogueScience Dr.Web	280	1953.3	[1]	14	5666.7		102	1562.9	18	4144.9
Eset NOD32	59	9270.0		7	11333.4		40	3985.4	5	14921.5
FRISK F-Prot Antivirus	89	6145.3		5	15866.8		57	2796.8	6	12434.6
F-Secure Anti-Virus	204	2681.0		9	8814.9		107	1489.9	18	4144.9
GDATA AntiVirusKit	425	1286.9	1	18	4407.4		210	759.1	30	2486.9
Grisoft AVG	126	4340.7	[6]	8	9916.7		50	3188.3	10	7460.7
Kaspersky KAV	126	4340.7		13	6102.6		82	1944.1	22	3391.2
MicroWorld eScan	140	3906.7		20	3966.7		81	1968.1	27	2763.2
NAI McAfee VirusScan	92	5944.9		15	5288.9		64	2490.9	20	3730.4
Norman Virus Control	68	8043.1	1	7	11333.4		63	2530.4	13	5739.0
NWI VirusChaser	168	3255.5	[12]	9	8814.9		61	2613.4	10	7460.7
SOFTWIN BitDefender	1576	347.0	[2]	8	9916.7		602	264.8	16	4663.0
Sophos Anti-Virus	59	9270.0		9	8814.9		44	3623.1	11	6782.5
Symantec SAV	126	4340.7		19	4175.5		61	2613.4	19	3926.7
Trend ServerProtect	57	9595.3		4	19833.4		28	5693.4	6	12434.6
VirusBuster VirusBuster	195	2804.8		7	11333.4		125	1275.3	16	4663.0

Being based on *Dr.Web*, *VirusChaser* shares the fussiness over changing on-access settings which characterises that program. Unfortunately *VirusChaser* also has fewer options available for the on-access scanner, thus making it more difficult to achieve the optimal settings for, among other things, testing. Since file-blocking on detection was not supported, in the end the collection was XCOPYed and logs used. Logs are not the preferred method for on-access scanning since, in my experience, they have a disturbing tendency to have missing entries. *VirusChaser's* detection rate was distinctly sub-standard to that of the parent product. BAT/Mumu.A was missed both on access and on

demand, and although no true false positives were seen, there were numerous suspicious files in the clean set.

SOFTWIN BitDefender Standard Edition 7.1

ItW Overall	100.00%	Macro	99.69%
ItW Overall (o/a)	100.00%	Standard	99.01%
ItW File	100.00%	Polymorphic	96.50%

With two suspicious files in the clean set, *BitDefender's* start was not awful, but certainly ripe for improvement. Sure

enough detection rates were good, and the lack of any true false positives merited a VB 100% award. Once again *BitDefender* achieved the slowest scanning rates in the review, though this situation should not last long. The developers noted that, in their tests, scanning speed was far more reasonable and that some of VB's files might be causing the problems. With the aid of a few logs it seems likely that *SOFTWIN* will be able to trim these times considerably.



Sophos Anti-Virus 3.74

ItW Overall	100.00%	Macro	99.80%
ItW Overall (o/a)	100.00%	Standard	99.49%
ItW File	100.00%	Polymorphic	98.06%

After having suffered in the polymorphics from the eternal affliction of ACG non-detection, *SAV* is now able to root out these infections in their entirety. Not only do I have fewer numbers to input as a result of this, but the folk at *Sophos* can also feel suitably relieved. Some things do not change however. All the criteria for a VB 100% award were easily achieved by *SAV*, and thus one wends its way to them through the figurative ether.



Symantec SAV Corporate Edition 8.1.0.25

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

Symantec AntiVirus's detection of all viruses in the test set, combined with the usual lack of false positives, earned *SAV* another VB 100% award. Scans of the on-demand test sets took over four hours, in comparison with four minutes as a more typical time for some products. This is really only a problem if you have a massive infection problem prior to installing *SAV*, though in this situation desperation to be uninfected might well overcome any care for speed. On the clean files no such speed problems were noted.



Trend Micro ServerProtect 5.56 Build (1007)

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.85%
ItW File	100.00%	Polymorphic	94.38%

ServerProtect was unique among the programs on offer in requiring to be set up in a domain with an active domain

controller. It also needs to be set up with a distribution server, making it pre-configured for network updates and upgrades, but total overkill on a single machine. It also causes considerable issues when attempting to update with standard definitions rather than, directly or indirectly, through a net connection. Then again, anyone using a *Windows 2003 Web Edition Server* on its own has rather more problems to contend with already. It came as a great surprise that logging seemed constrained by the amount of data that could be processed at any one time. Due to the methods used to store the data, the information concerning a scan of 25,000 viruses seemed to take up rather more than 50 MB. This information was too great for the log parser to assimilate, thus logs were truncated when exported. As a result testing was performed by deletion. With these niggles out of the way, scanning was speedy and detection good, though slightly weak on polymorphics. With no false positives, *Trend's* VB 100% award is well deserved.



VirusBuster VirusBuster 4.4 Build 2

ItW Overall	100.00%	Macro	100.00%
ItW Overall (o/a)	100.00%	Standard	99.82%
ItW File	100.00%	Polymorphic	91.45%

The final product in the review is again one which performs too well for any lovingly crafted words of vitriol to be appropriate. *VirusBuster* continues to show sturdy detection and with no false positives is due a VB 100%.



CONCLUSION

Overall the review held in store more surprises than I had expected; the problems relating to the new OS were fewer and the traditional problems were more profound than I thought likely. Although those companies who suffered may not find it particularly comforting, the pain of upgrading from one OS to another seems to be lessening overall. Not that this should be a concern for a couple of years yet – with the next generation of *Windows* looking increasingly likely to be delayed further, system patches rather than replacements will more than likely be the order of the day.

Technical details:

Test environment: Identical 1.6 GHz Intel Pentium machines with 512 MB RAM, 20 GB dual hard disks, DVD/CD-Rom and 3.5-inch floppy drive running *Windows Server 2003 Web Edition V5.2 Build 3790*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win2K/2003/test_sets.html.