COMPARATIVE REVIEW

WINDOWS SERVER 2003 ENTERPRISE X64 VERSION

Matt Ham

Over the last year I have received an increasing number of enquiries, from both product developers and end users, as to when *Virus Bulletin* would produce a review on a 64-bit operating system. This comparative review comes as a result of that interest.

With 64-bit systems there is a range of hardware available, with operating systems to match. Having asked a selection of vendors and end users, it seems that *Athlon 64* processors are the most commonly used with 64-bit operating systems and thus were chosen as a hardware platform. *Windows Server 2003 x64* version was selected as the operating system, again based on reports received from a number of vendors and end users.

The biggest surprise in the review was the lack of submissions. I was certainly expecting a smaller number of products to be submitted for this test than for the previous *Windows 2003 Server* review, but for numbers to drop to just over a third was more extreme than expected. Whether other products were missing due to corporate cowardice or known incompatibilities with the platform I will leave to the reader to imagine.

TEST SETS

With hardware and operating systems already changed drastically it seemed unwise to make major changes to the test sets too. In the event, the most recent WildList available at the start of the test period was that from July 2005 – only one month newer than the one used in October's *Windows Server 2003* comparative review (see *VB*, October 2005, p.12). All the products included in this review were also tested on that occasion. Products were dated no later than 31 October 2005.

That is not to say that there wasn't a great temptation to add new samples to both clean and infected test sets on this occasion. The clean test sets in particular are perhaps unrepresentatively high in dynamic archives, which slow on-demand scan speeds more than would be seen in most real-world settings. Both test sets will be updated considerably between now and mid-2006 – and had there not already been so many other major changes this month, the process would already have begun.

Since this was the first outing of this hardware, the throughput tests cannot be compared directly with past results. In future reviews the hardware is likely to vary between tests, so care should be taken to ensure than any comparison is meaningful.

Some clarification has been requested as to the way in which our tests are performed where archives are concerned. In all cases the non-archive clean test sets are scanned using the product's default settings. In some cases, however, the product's default settings do not include the scanning of ZIP archives. For these products archive scanning is activated during the archive throughput tests, but not at any other time. This avoids creating the illusion of those products with no default archive scanning having astoundingly speedy throughput on archives.

Archive scanning becomes more of a thorny issue where dynamic archives are concerned. A product which does not scan such files will have a distinct advantage in scanning the clean test set over a product where such a setting is off by default. This is a genuine real-world difference, although, as mentioned above, the throughput results are somewhat biased towards products with either very fast or non-existent handling of dynamically compressed executables.

Alwil avast! 4.6.511

ItW Overall	100.00%	**Macro**	99.56%
ItW Overall (o/a)	100.00%	**Standard**	99.36%
ItW File	100.00%	**Polymorphic**	93.57%

Avast!'s on-access scanner is still one of the more fussy with respect to what will cause a detection to be announced. As a result, detections were logged on access when copying files, rather than simply accessing the files. *Avast!* is also one of the products where ZIP scanning was activated for the purposes of archive throughput testing. *Avast!* began a fairly predictable trend in which products behaved almost exactly as they did in the previous *Windows 2003 Server* review. A VB 100% award was the result again.

CA eTrust Antivirus 7.1.192 (InoculateIT engine) 23.70 86

ItW Overall	100.00%	**Macro**	99.90%
ItW Overall (o/a)	100.00%	**Standard**	99.63%
ItW File	100.00%	**Polymorphic**	99.89%

Although supplied as part of the standard *eTrust* package, the *InoculateIT* engine is not the default for this product, and as a result does not qualify for a VB 100% award – the results are presented here purely for interest. True to recent form, the product put in a very good performance, with all infected files In the Wild detected as such.

On-access tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	112	93.58%	17	99.18%
CA eTrust Antivirus (I)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	4	99.51%
CA eTrust Antivirus (V)	0	100.00%	0	100.00%	100.00%	12	99.82%	1	99.95%	3	99.84%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	82	98.04%	313	96.25%	147	93.06%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
GDATA AntiVirusKit	0	100.00%	3	0.00%	99.55%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	0	100.00%	257	85.97%	30	98.41%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	2	99.88%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	29	97.67%	0	100.00%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%

CA eTrust Antivirus 7.1.192 (Vet engine) 11.9 9487

ItW Overall	100.00%	**Macro**	99.82%
ItW Overall (o/a)	100.00%	**Standard**	99.96%
ItW File	100.00%	**Polymorphic**	99.95%

While the log files for both the incarnations of *eTrust* continue to be the epitome of uselessness, the product itself performs well in both throughput and detection tests. A VB 100% award is the result, even though it would not be readily apparent from normal scrutiny of the aforementioned logs.

CAT Quick Heal 8.00 SP1

ItW Overall	100.00%	**Macro**	98.18%
ItW Overall (o/a)	100.00%	**Standard**	96.48%
ItW File	100.00%	**Polymorphic**	96.25%

This submission was designated the server version of the product, which in many other cases tends to result in a rather complex installation procedure.

Quick Heal proved to be at quite the opposite end of the spectrum, with perhaps the fastest install procedure of any GUI-based anti-virus program I have reviewed. Scanning too was relatively rapid and resulted in detection of all the samples in the In the Wild (ItW) test sets – both on demand and on access. It comes as no surprise that this performance is rewarded with a VB 100%.

ESET NOD32 1.1268(20051031)

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

Having been tested in a comparative review two months ago and a standalone review in last month's issue of the magazine (see *VB*, November 2005, p.16), no great surprises were expected from *NOD32*. *NOD32* has ZIP archive scanning turned off by default, although W32/Heidi.A is detected by the engine as a special case, accounting for full detection of this virus in the standard test set. In any case detection was at its usual high levels for this product, and *NOD32* obtains a VB 100% award for its collection as a result.

GDATA AntiVirusKit 16.0.3

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	99.55%	**Standard**	100.00%
ItW File	100.00%	**Polymorphic**	100.00%

GDATA's product is one which has suffered a little in the past from sluggish scanning – a result of the fact that it has two scanning engines which are both in use in each scan. However, the additional raw power of the new hardware in

use here made this less noticeable during testing. The file-based part of the testing was a definite success for *AVK*, with all infected files detected both on access and on demand. However, scanning of floppies on access proved less of a triumph. No detection could be triggered in any log, and no alerts were generated for infected disks. Whether this was due to the change in platform or hardware will no doubt be a point of investigation for the *GDATA* developers. *AVK* thus fails to obtain a VB 100% award on this occasion.

Grisoft AVG Anti-Virus 7.1.362

ItW Overall	100.00%	**Macro**	100.00%
ItW Overall (o/a)	100.00%	**Standard**	98.56%
ItW File	100.00%	**Polymorphic**	85.97%

The installation files for *AVG* are the same across all recent *Windows* platforms, with no reboot required before installation is declared complete. As usual, however, the machine was rebooted after installation as part of the standard test regime. The scanner detected all files in the ItW test set as in previous tests. With no false positives, *AVG* is worthy of a VB 100%. Indeed the whole test was notable for the fact that no false positives were generated.

Kaspersky Anti-Virus 5.0.70.0

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

The *Kaspersky* product tested here was the command line scanner, the optional GUI being left for examination in future. The on-demand scanner still seemed to be a little slower than expected when scanning infected files. However, this was only in comparison with *Kaspersky*'s usual rapid throughput, its speed of scanning coming nowhere close to slow overall.

With one hundred per cent detection on demand, and very close to this on access (including full detection of all ItW samples), a VB 100% award is on its way to Moscow.

McAfee VirusScan Enterprise 8.0.0 4616 4400

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

The biggest niggle with *VirusScan* is the highly involved process that is required to set up new scans, however this is gradually showing signs of improvement. Oddly, on this occasion, changing and saving the settings resulted in a second prompt to save when the task was closed.

Scanning completed with no problems at all and detection rates were very good as expected – all files being detected in the on-demand scan of infected objects. Files missed on access included several samples of W32/Etap, presumably due to the complexity of these files causing a time-out

On-demand tests	ItW File		ItW Boot		ItW Overall	Macro		Polymorphic		Standard	
	Number missed	%	Number missed	%	%	Number missed	%	Number missed	%	Number missed	%
Alwil avast!	0	100.00%	0	100.00%	100.00%	18	99.56%	113	93.57%	15	99.36%
CA eTrust Antivirus (I)	0	100.00%	0	100.00%	100.00%	4	99.90%	1	99.89%	2	99.63%
CA eTrust Antivirus (V)	0	100.00%	0	100.00%	100.00%	12	99.82%	1	99.95%	1	99.96%
CAT Quick Heal	0	100.00%	0	100.00%	100.00%	75	98.18%	313	96.25%	100	96.48%
Eset NOD32	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
GDATA AntiVirusKit	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Grisoft AVG	0	100.00%	0	100.00%	100.00%	0	100.00%	257	85.97%	27	98.56%
Kaspersky KAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
McAfee VirusScan	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	100.00%
Symantec SAV	0	100.00%	0	100.00%	100.00%	0	100.00%	0	100.00%	0	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)
Alwil avast!	56.0	9766.6	0	13	6102.6	0	45	3542.6	14	5329.1
CA eTrust Antivirus (I)	53.0	10319.5	0	2	39666.9	0	21	7591.3	4	18651.9
CA eTrust Antivirus (V)	44.0	12430.3	0	1	79333.8	0	23	6931.2	4	18651.9
CAT Quick Heal	38.0	14393.0	0	6	13222.3	0	22	7246.2	6	12434.6
Eset NOD32	18.0	30385.1	0	2	39666.9	0	13	12262.8	3	24869.2
GDATA AntiVirusKit	194.0	2819.2	0	7	11333.4	0	74	2154.3	10	7460.7
Grisoft AVG	75.0	7292.4	0	3	26444.6	0	28	5693.4	4	18651.9
Kaspersky KAV	85.0	6434.5	0	8	9916.7	0	40	3985.4	9	8289.7
McAfee VirusScan	42.0	13022.2	0	5	15866.8	0	27	5904.3	6	12434.6
Symantec SAV	79.0	6923.2	0	7	11333.4	0	33	4830.8	5	14921.5

somewhere in scanning. *VirusScan* also required the scanning of ZIP files to be activated for the archive clean set tests. With full detection of all samples in the ItW test sets, however, a VB 100 % award is the result.

Symantec AntiVirus 10.0.0.359 103.0.2.7

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

Things got off to a bad start with *SAV*, the initial package supplied being for the *Itanium* processor rather than the *AMD* used in the tests. *Symantec* has discontinued support for *Itanium* processors in *SAV 10*, so this should not be a problem in future.

More of an issue, however, was the speed at which infected files were scanned on demand. At around four seconds per file, this was over 1,000 times slower than some of the other products on test. In fact, even the total scan times of all other tests performed during the course of the review did not reach that of *SAV*'s single on-demand scan. The problem seemed to be linked in some way to the GUI, since on-access scanning proceeded at a far more reasonable speed. What is more, after a large number of infected files had been scanned on demand, the load and unload times of the GUI rose to close to five minutes each.

The *SAV* log file continues to seem to be the product of a madman or a fool – for example, several samples of W97M/AntiSocial.F were logged under the highly useful file name of '??????'. Needless to say, this is not a name which any of the samples possess, the real name of this file being ANTI_F-1.DOC.

However, *SAV* did manage to detect all the samples in the ItW test sets, and despite the fact that I have had more pleasurable dentistry, a VB 100% is awarded to this product.

CONCLUSIONS

In the aftermath of the tests it has become clear that the tales of woe I had heard concerning 64-bit operating systems were, at least as far as anti-virus software is concerned, somewhat exaggerated. Installation of the operating system and drivers proceeded without a hitch and the same was true for the majority of the products on test. In many cases the product submitted was exactly the same as that supplied for the previous test, the installation packages combining 64-bit and 32-bit versions of the application.

After such a painless review I expect the next 64-bit comparative review in these pages to be graced with a rather larger number of entrants.

Technical details

Test environment: Identical AMD Athlon 64 3800+ dual core machines with 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, running *Microsoft Windows Server 2003 Enterprise X64 version*, *Service Pack 1*.

Virus test sets: Complete listings of the test sets used are at http://www.virusbtn.com/Comparatives/Win64/2005/test_sets.html.

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