# COMPARATIVE REVIEW

## WINDOWS 2003 ADVANCED SERVER

*Matt Ham*

With *Windows Longhorn* now renamed *Windows Vista*, and still not expected for years, *Windows 2003 Server* remains the most recent server platform at the moment and for the foreseeable future. Having been in production for several years now, I expected the tests to progress easily on this occasion, since mature platforms tend to be less prone to problems. In the event, however, a host of problems were encountered. Some of these were due to the efficiency of the products, though rather more were the result of questionable design decisions.

### TEST SETS

The products included in this month's review were required to have publication dates no later than 31 August 2005 (both for the product itself and any database updates). The test sets were aligned with the most recent WildList published at the time, which was the June 2005 edition.

As expected, the bulk of additions to the test sets were W32/Mytob variants. This worm was of note more for its vast number of variants than the overwhelming success of any particular specimen – over 100 variants were added to the test sets. The majority of additional samples within the WildList (and added to the In the Wild [ItW] test set) were worms of one sort or another.

With the addition of the horde of W32/Mytob variants to the test sets, one feature of the scanners which would be of particular interest was their ability to use efficient generic detection techniques. All in all, however, there were no great challenges in terms of detection.

As a special note, when performing throughput tests on the zipped clean sets, most products were set up so as to detect within archives in their default state. The other products were activated for archive scanning during these tests alone. The products where archives are not scanned by default are those produced by *AhnLab*, *Eset*, *McAfee*, *Sophos* and *VirusBuster*.

### AhnLab V3Net 6.0 2005.08.31.10

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 98.97% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 90.61% |
| **ItW File** | 100.00% | **Polymorphic** | 46.52% |

The only major problem encountered with *AhnLab*'s offering was with the logs produced during on-demand scanning. These note only the file name on a single line, rather than the full path, thus making analysis lengthy. However, this problem does not affect detection rate and is likely to be of little relevance for most users. Of much more importance are the matters of detection and false positives, both areas where *V3Net* performed sufficiently well to be awarded a VB 100%.


### Alwil avast! 4.6.497

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.56% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.38% |
| **ItW File** | 100.00% | **Polymorphic** | 93.57% |

With absolutely no problems or outstanding issues in its operation, *avast!* is destined for a rather uneventful write-up in this review. A VB 100% award will, one hopes, go some way towards making up for the lack of discussion concerning the product.


### Authentium Command AntiVirus 4.93.0

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 100.00% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.72% |
| **ItW File** | 100.00% | **Polymorphic** | 100.00% |

Again, the performance of *Command AntiVirus* produced nothing to comment on other than the full detection of viruses in the ItW set and the lack of false positives. Instead I will content myself with congratulating *Authentium* on achieving a further VB 100% for its collection.


### Avira Avira for Windows Server 1

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

Having detected all samples in all of the test sets in the last *Windows* review, *Avira* will be pleased to have repeated the performance on this occasion. The fact that false positives are counted only in the non-archived clean test sets turned out to be fortuitous for *Avira*, since one clean archive was declared to contain a sample of W32/Fosforo.


Scanning was otherwise a little slow but uneventful and a VB 100% award is thus winging its way to *Avira*'s headquarters.

## CA eTrust Antivirus (InoculateIT engine) 7.1.192 23.70.24

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.90% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.61% |
| **ItW File** | 100.00% | **Polymorphic** | 99.89% |

*eTrust AntiVirus* is provided with two scanning engines which can be exchanged at will: one can be used for on-access and the other for on-demand scanning if so desired. The *InoculateIT* engine is not activated by default, though, and is thus not eligible for a VB 100% award. It did, however, detect all samples in the wild, with no false positives.

## CA eTrust Antivirus (default Vet engine) 7.1.192 11.9.9371

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.82% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.84% |
| **ItW File** | 100.00% | **Polymorphic** | 99.95% |

The *Vet* engine in the *eTrust* product performed slightly better in terms of detection than its optional counterpart, while speed tests produced similar results. Customers should therefore find little to complain about over the choice of default engine. Likewise, *CA*'s developers will be unlikely to complain at receiving a VB 100% award for their efforts.

## CA Vet Anti-Virus 10.67.0.0 11.9.1.0 9371

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

The strangest thing to happen while testing *Vet* was the production, during the installation procedure, of a dialog which read 'Should not see me' while the machine was rebooting. That apart, detection and false positives were much the same here as when the engine was tested in its *eTrust* incarnation. A second VB 100% for a product based on *Vet*'s engine is the result.

## CAT Quick Heal 2006 8.00

| | | | |
|---|---|---|---|
| **ItW Overall** | 99.97% | **Macro** | 98.27% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 96.12% |
| **ItW File** | 99.97% | **Polymorphic** | 96.23% |

*Quick Heal* has established itself in *VB*'s tests as a reliable regular which tends to produce no major problems in testing. I appreciated this more than usual on this occasion, since I managed to lose my initial results for *Quick Heal* and was forced to repeat the tests. The overall result was identical, with a VB 100% narrowly missed on both occasions. The offending file was a .EML sample of W32/Nimda.A, missed on demand.

## Dr.Web Dr.Web 4.33.0.08190

| | | | |
|---|---|---|---|
| **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*'s detection rates have always been high, with a handful of misses in the last few tests being attributable to optimization of older virus detections. On this occasion the optimizations were clearly working well, since all samples were detected in all test sets. A continuing irritation is this product's on-access scanner, which although still requiring a reboot for any configuration changes, no longer announces this fact. Irritation aside, a VB 100% is well deserved by the product.

## Eset NOD32 1.1207

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

*NOD32* has a strong history of detecting all infected files, with only a few minor deviations over the years. Yet again, no infected samples were missed across this month's test sets. A VB 100% award for *Eset* is the predictable result.

## Fortinet FortiClient 2.0.110

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.39% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 98.84% |
| **ItW File** | 100.00% | **Polymorphic** | 97.04% |

*Fortinet*'s product is beginning to become a familiar subject in *VB*'s tests and its scanning results reflect this, with further improvements likely in the future. A VB 100% is awarded to *FortiClient* – which is also starting to become a regular result for the product.

| On-demand tests | ItW File | | ItW Boot | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number missed | % | Number missed | % | % | Number missed | % | Number missed | % | Number missed | % |
| AhnLab V3Net | 0 | 100.00% | 0 | 100.00% | 100.00% | 47 | 98.97% | 8834 | 46.52% | 191 | 90.61% |
| Alwil avast! | 0 | 100.00% | 0 | 100.00% | 100.00% | 18 | 99.56% | 113 | 93.57% | 14 | 99.38% |
| Authentium Command | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 2 | 99.72% |
| Avira Avira | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| CA eTrust Antivirus (I) | 0 | 100.00% | 0 | 100.00% | 100.00% | 4 | 99.90% | 1 | 99.89% | 3 | 99.61% |
| CA eTrust Antivirus (V) | 0 | 100.00% | 0 | 100.00% | 100.00% | 12 | 99.82% | 1 | 99.95% | 3 | 99.84% |
| CA Vet Anti-Virus | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 1 | 99.95% | 1 | 99.96% |
| CAT Quick Heal | 1 | 99.97% | 0 | 100.00% | 99.97% | 71 | 98.27% | 317 | 96.23% | 106 | 96.12% |
| Dr.Web Dr.Web | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Eset NOD32 | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Fortinet FortiClient | 0 | 100.00% | 0 | 100.00% | 100.00% | 31 | 99.39% | 73 | 97.04% | 38 | 98.84% |
| FRISK F-Prot Antivirus | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 2 | 99.72% |
| 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% |
| Grisoft AVG | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 257 | 85.97% | 27 | 98.56% |
| H+BEDV AntiVir | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Hauri ViRobot | 0 | 100.00% | 0 | 100.00% | 100.00% | 12 | 99.71% | 9 | 99.76% | 15 | 99.17% |
| 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% |
| MicroWorld eScan | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Norman Virus Control | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 180 | 91.24% | 8 | 99.62% |
| SOFTWIN BitDefender | 0 | 100.00% | 0 | 100.00% | 100.00% | 34 | 99.12% | 5 | 99.78% | 17 | 99.27% |
| Sophos Anti-Virus | 1 | 99.84% | 0 | 100.00% | 99.84% | 8 | 99.80% | 0 | 100.00% | 15 | 99.30% |
| Symantec SAV | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Trend Micro Server Protect | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 215 | 95.77% | 6 | 99.39% |
| UNA UNA | 3 | 99.53% | 0 | 100.00% | 99.53% | 1891 | 55.06% | 13008 | 24.40% | 433 | 80.43% |
| VirusBuster VirusBuster | 0 | 100.00% | 0 | 100.00% | 100.00% | 7 | 99.88% | 171 | 92.29% | 28 | 98.88% |

## FRISK F-Prot AntiVirus 3.16c

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 100.00% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.72% |
| **ItW File** | 100.00% | **Polymorphic** | 100.00% |

Unusually, several more files were missed by *F-Prot* while scanning on access than were missed on demand. *FRISK*'s development team will no doubt be looking into this, although the problems did not occur in the ItW test sets, rather among very much older samples. Therefore, with no

false positives generated, a VB 100% makes its way to Iceland for *F-Prot*.

## F-Secure Anti-Virus 5.50 11110

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

*F-Secure*'s product has had a number of uncharacteristic non-detections in some recent tests, but the product's detection rate returned to its usual high levels in this test, and with no false positives a VB 100% is the result.


## GDATA AntiVirusKit 15.0.5 16.230

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

With its combination of two engines, *AVK* has sometimes seemed slightly slow while scanning, though on this occasion speed problems were comparatively non-existent. The engine combination has also traditionally paid off with good detection rates and in this there was no change – all infected files being detected in all test sets. With no false positives, the product qualified easily for a VB 100%.


## Grisoft AVG Anti-Virus 7.00 344

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

Unfortunately *AVG* generated one false positive while scanning the clean set this month. Despite good performance in all the detection-based tests this was sufficient to prevent *Grisoft*'s product from achieving a VB 100% this time.

## H+BEDV AntiVir 6.31.1.0

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

Since *AntiVir* is all but identical to *Avira*, it came as no great surprise that the scanning results for the two products were identical – all infections were detected as such. Scanning speeds were also very similar, with differences easily attributable to those induced by background OS activity. Like its twin product, therefore, *AntiVir* gains a VB 100% award.


## Hauri ViRobot 2005-08-24.00

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.71% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.17% |
| **ItW File** | 100.00% | **Polymorphic** | 99.76% |

*ViRobot* started the testing process disappointingly, with three false positives being picked up in the clean set. The scanning of infected files was, if anything, more frustrating, since numerous files took well over a minute to be scanned. Scanning of the test set rapidly became slower during the process, with a virtual memory warning also occurring. This combination suggests that bad things are afoot. It also seemed that exclusions were totally non-functional, requiring the product to be fully uninstalled for any manipulation of infected files to occur. It was perhaps not surprising that many files were missed on access, presumably due to timeouts during scanning.

## Kaspersky Anti-Virus 5.0.50.0

| | | | |
|---|---|---|---|
| **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* entry this month was a great surprise, consisting of a command line scanner rather than the usual GUI. An optional 'free' GUI was suggested to interface with this. However, the interface required a fully operational SQL database to be installed on the machine in question. While many servers will have SQL available, those which do not will require a new installation which is free neither in a financial sense nor in a manpower sense. Oddly enough the command line version seemed, by pure observation, to be slower at scanning infected files than the more usual GUI versions tested. All these oddities aside, *KAV* receives a VB 100% award.


## McAfee VirusScan Enterprise 8.0.0 4400 4571

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

The greatest surprise when testing *VirusScan* was noted during on-access scanning, where many samples of W32/Etap were not detected. It is possible that timeouts are responsible for this behaviour. W32/Etap is not a member of the ItW test set, however, so these obscure missed detections still allow *McAfee* to take home a VB 100% award for its pains.

## MicroWorld eScan Win 1.27

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

*MicroWorld*'s *eScan* is part of a suite of, at least in some cases, rebadged products covering a variety of security functions. The anti-virus is provided by a version of *GDATA*'s *AVK*, which, as in its original form, detected all samples that passed its way. It will come as little surprise, therefore, that a VB 100% is awarded to *MicroWorld*.

## Norman Virus Control 5.81

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 100.00% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.62% |
| **ItW File** | 100.00% | **Polymorphic** | 91.24% |

*Norman*'s product remains a solid workhorse, the only real complaint being that the scanning throughput is somewhat low. This is not the gravest of sins, however, and other areas of performance were sufficiently good that a VB 100% award is the result.

## SOFTWIN BitDefender 2.0.172

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.12% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.27% |
| **ItW File** | 100.00% | **Polymorphic** | 99.78% |

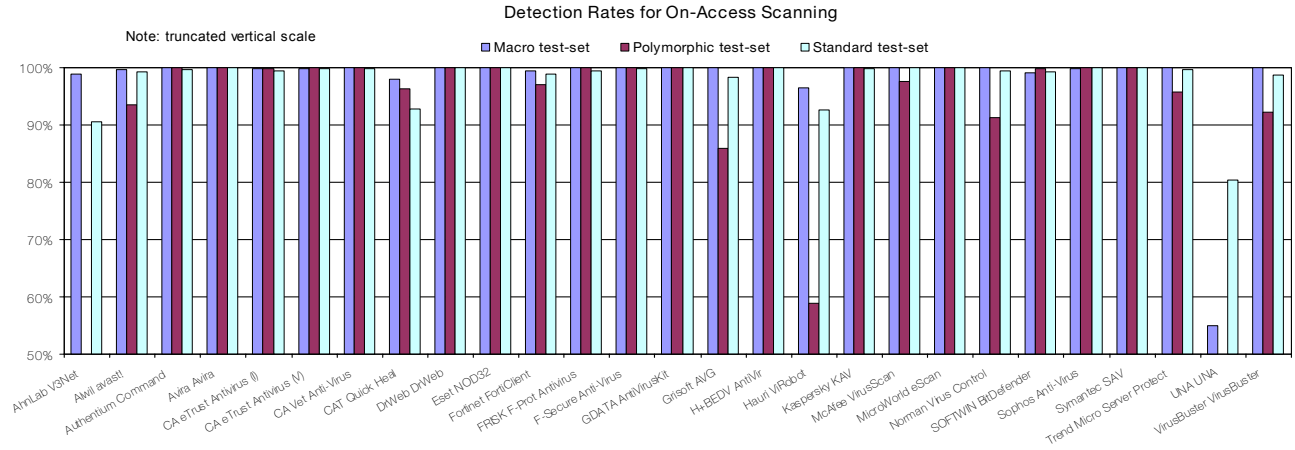
A notable change in this version of *BitDefender* is the interface, which is much more akin to MMC than a usual anti-virus GUI. This added some initial frustration to the process of scanning, though once the changes had become less unfamiliar, the frustration was substantially lessened. With novelty present in the interface, the underlying scanning capacity of the program remains similar. As a result a VB 100% award is appropriate.

## Sophos Anti-Virus 5.0.5

| | | | |
|---|---|---|---|
| **ItW Overall** | 99.84% | **Macro** | 99.80% |
| **ItW Overall (o/a)** | 99.84% | **Standard** | 99.30% |
| **ItW File** | 99.84% | **Polymorphic** | 100.00% |

The new *Sophos* interface includes a quarantine function which has certain peculiarities. Having scanned the test sets on demand, the summary declared that there were over 20,000 items in the quarantine. A different area claimed that this total was 1,000, while inspecting the quarantine area itself showed that there were precisely zero files in that location.

There were also new occurrences during scanning. On access several files were detected on this occasion which have not been detected in any previous default scan. Unfortunately, both on access and on demand, a sample of W32/Sdbot was missed from the ItW test set, thus denying the product a VB 100% award.



| On-access tests | ItW File | | ItW Boot | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number missed | % | Number missed | % | % | Number missed | % | Number missed | % | Number missed | % |
| AhnLab V3Net | 0 | 100.00% | 0 | 100.00% | 100.00% | 47 | 98.97% | 8842 | 46.49% | 191 | 90.61% |
| Alwil avast! | 0 | 100.00% | 0 | 100.00% | 100.00% | 18 | 99.56% | 113 | 93.57% | 17 | 99.18% |
| Authentium Command | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 5 | 99.58% |
| Avira Avira | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| 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% |
| CA Vet Anti-Virus | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 1 | 99.95% | 3 | 99.84% |
| CAT Quick Heal | 0 | 100.00% | 0 | 100.00% | 100.00% | 82 | 98.04% | 313 | 96.25% | 156 | 92.72% |
| Dr.Web Dr.Web | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Eset NOD32 | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Fortinet FortiClient | 0 | 100.00% | 0 | 100.00% | 100.00% | 31 | 99.39% | 73 | 97.04% | 38 | 98.84% |
| FRISK F-Prot Antivirus | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 4 | 99.98% | 8 | 99.40% |
| 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% |
| Grisoft AVG | 0 | 100.00% | 0 | 100.00% | 100.00% | 3 | 99.93% | 257 | 85.97% | 30 | 98.41% |
| H+BEDV AntiVir | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Hauri ViRobot | 0 | 100.00% | 0 | 100.00% | 100.00% | 145 | 96.44% | 5358 | 58.94% | 112 | 92.61% |
| 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% |
| MicroWorld eScan | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% |
| Norman Virus Control | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 180 | 91.24% | 10 | 99.50% |
| SOFTWIN BitDefender | 0 | 100.00% | 0 | 100.00% | 100.00% | 34 | 99.12% | 5 | 99.78% | 17 | 99.27% |
| Sophos Anti-Virus | 1 | 99.84% | 0 | 100.00% | 99.84% | 8 | 99.80% | 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% |
| Trend Micro Server Protect | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 215 | 95.77% | 9 | 99.63% |
| UNA UNA | 3 | 99.53% | 0 | 100.00% | 99.53% | 1891 | 55.06% | 13008 | 24.40% | 433 | 80.43% |
| VirusBuster VirusBuster | 0 | 100.00% | 0 | 100.00% | 100.00% | 0 | 100.00% | 172 | 92.30% | 30 | 98.64% |

## Symantec AntiVirus 10.0.0.359

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

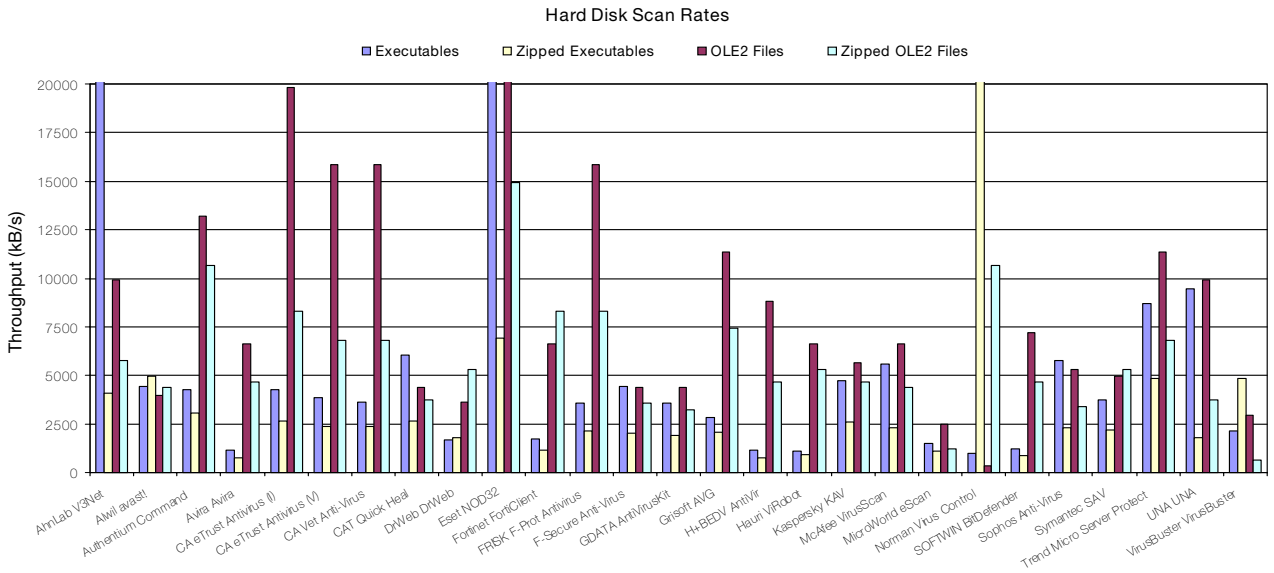
*Symantec*'s new engine seemed to bring few major changes to the process of scanning, and indeed none whatsoever in the results of those scans. With all infected files detected, however, an improvement would be hard to obtain and a VB 100% award impossible to deny.

| 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 | 26.0 | 21035.9 | | 8 | 9916.7 | | 39 | 4087.6 | 13 | 5739.0 |
| Alwil avast! | 123.0 | 4446.6 | | 20 | 3966.7 | | 32 | 4981.8 | 17 | 4388.7 |
| Authentium Command | 129.0 | 4239.8 | | 6 | 13222.3 | | 52 | 3065.7 | 7 | 10658.2 |
| Avira Avira | 465.0 | 1176.2 | | 12 | 6611.1 | | 221 | 721.3 | 16 | 4663.0 |
| CA eTrust Antivirus (I) | 128.0 | 4272.9 | | 4 | 19833.4 | | 60 | 2656.9 | 9 | 8289.7 |
| CA eTrust Antivirus (V) | 142.0 | 3851.6 | | 5 | 15866.8 | | 68 | 2344.4 | 11 | 6782.5 |
| CA Vet Anti-Virus | 150.0 | 3646.2 | | 5 | 15866.8 | | 68 | 2344.4 | 11 | 6782.5 |
| CAT Quick Heal | 90.0 | 6077.0 | | 18 | 4407.4 | | 60 | 2656.9 | 20 | 3730.4 |
| DrWeb DrWeb | 325.0 | 1682.9 | | 22 | 3606.1 | | 90 | 1771.3 | 14 | 5329.1 |
| Eset NOD32 | 27.0 | 20256.7 | | 3 | 26444.6 | | 23 | 6931.2 | 5 | 14921.5 |
| Fortinet FortiClient | 315.0 | 1736.3 | | 12 | 6611.1 | | 140 | 1138.7 | 9 | 8289.7 |
| FRISK F-Prot Antivirus | 154.0 | 3551.5 | | 5 | 15866.8 | | 74 | 2154.3 | 9 | 8289.7 |
| F-Secure Anti-Virus | 124.0 | 4410.7 | | 18 | 4407.4 | | 78 | 2043.8 | 21 | 3552.7 |
| GDATA AntiVirusKit | 152.0 | 3598.2 | | 18 | 4407.4 | | 85 | 1875.5 | 23 | 3243.8 |
| Grisoft AVG | 195.0 | 2804.8 | 1 | 7 | 11333.4 | | 77 | 2070.3 | 10 | 7460.7 |
| H+BEDV AntiVir | 470.0 | 1163.7 | | 9 | 8814.9 | | 217 | 734.6 | 16 | 4663.0 |
| Hauri ViRobot | 506.0 | 1080.9 | 3 | 12 | 6611.1 | | 172 | 926.8 | 14 | 5329.1 |
| Kaspersky KAV | 116.0 | 4714.9 | | 14 | 5666.7 | | 62 | 2571.2 | 16 | 4663.0 |
| McAfee VirusScan | 98.0 | 5580.9 | | 12 | 6611.1 | | 70 | 2277.4 | 17 | 4388.7 |
| MicroWorld eScan | 366.0 | 1494.4 | | 32 | 2479.2 | | 148 | 1077.1 | 62 | 1203.3 |
| Norman Virus Control | 545.0 | 1003.5 | | 222 | 357.4 | | 6 | 26569.4 | 7 | 10658.2 |
| SOFTWIN BitDefender | 460.0 | 1189.0 | | 11 | 7212.2 | | 189 | 843.5 | 16 | 4663.0 |
| Sophos Anti-Virus | 95.0 | 5757.2 | | 15 | 5288.9 | | 70 | 2277.4 | 22 | 3391.2 |
| Symantec SAV | 147.0 | 3720.6 | | 16 | 4958.4 | | 72 | 2214.1 | 14 | 5329.1 |
| Trend Micro Server Protect | 63.0 | 8681.5 | | 7 | 11333.4 | | 33 | 4830.8 | 11 | 6782.5 |
| UNA UNA | 58.0 | 9429.9 | | 8 | 9916.7 | | 88 | 1811.6 | 20 | 3730.4 |
| VirusBuster VirusBuster | 257.0 | 2128.1 | 2 | 27 | 2938.3 | | 33 | 4830.8 | 120 | 621.7 |

## Trend Micro Server Protect 5.58.0.1060 7.510-1002 2.811.00

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 100.00% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 99.39% |
| **ItW File** | 100.00% | **Polymorphic** | 95.77% |

As has been the case with *Trend*'s server products for some time, *Server Protect* needed to be within a domain for installation. My main complaint, however, was with the log file, which seemed to be truncated to the point of uselessness. This was bypassed by setting the scanner to delete infected objects, rather than relying on parsed logs for detection calculations. *Server Protect* missed no ItW files and produced no false positives, therefore receives a VB 100%.




## UNA UNA PRO 1.83 269

| | | | |
|---|---|---|---|
| **ItW Overall** | 99.53% | **Macro** | 55.06% |
| **ItW Overall (o/a)** | 99.53% | **Standard** | 80.43% |
| **ItW File** | 99.53% | **Polymorphic** | 24.40% |

The user interface of this product has changed slightly since the last time it was reviewed, offering an easier and more pleasant experience on this front. There was also an improvement in detection rates, although misses of ItW samples were still present, thus denying *UNA* a VB 100%.

## VirusBuster VirusBuster 2005 5.0.175

| | | | |
|---|---|---|---|
| **ItW Overall** | 100.00% | **Macro** | 99.88% |
| **ItW Overall (o/a)** | 100.00% | **Standard** | 98.88% |
| **ItW File** | 100.00% | **Polymorphic** | 92.29% |

Unfortunately for *VirusBuster*, two false positives were noted in the clean test set and a VB 100% award was denied for this reason. *VirusBuster* is unusual in that it can use MMC as an interface for control. Control through MMC, however, seems not to allow the choice of areas to scan. A standard GUI is also available, with control here being irritatingly long-winded, but allowing the selection of scan areas.

## CONCLUSION

For such a stable and standard platform it was something of a surprise that so many problems showed themselves during testing. The usual caveat applies: that our test scenarios tend to throw more infected files at the scanners than might be expected in the real world. In the case of a server-based scanner, however, the loads produced by our tests might very well be reproduced in the case of a major outbreak, and under such circumstances some of the products tested here would be worthless. Scanning files at a rate of less than one per minute is far too slow and a server crippled by the load of scanning infected objects will prove more of a frustration than a useful tool.

Apart from the cries of woe brought about by these technical problems, design decisions also took their toll on my sanity. In a disturbingly high percentage of the products, the interface has been substantially changed for the worse over the last year. The most common irritation was the length of time required to set up a scan, for example, of a single directory. However much the design gurus may suggest otherwise, it is counterproductive to spend several minutes producing a detailed scan setup for an object, which will never be used again. Certainly complex feature tweaking should be a possibility, but making it a necessity is fundamentally user-unfriendly.

**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/2005/test_sets.html.

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

## ERRATA – WINDOWS 2003 SERVER COMPARATIVE REVIEW


Regrettably, there were three errors in the latest Windows 2003 Advanced Server comparative review (see *VB*, October 2005, p.12). In alphabetical order these were:

*CAT Quick Heal*: Initially this was flagged as having missed a sample of W32/Nimda.A in the .EML format. Subsequent tests revealed that the infected contents of the .EML file were removed, though the file itself remained. This must therefore be considered a detection and a VB 100% award is due to *Quick Heal*.

*MWI VirusChaser*: Due to an administrative error the tests for this product were omitted from the initial review. The product gained a VB 100% award when tested, with full detection in the wild and no false positives.

*Sophos Anti-Virus*: The product submitted by *Sophos* was that which was available to the public on the company's website at the time of the review submission. Due to miscommunication, however, the versions downloaded for testing, were an incompatible combination of base scanning engine and virus database updates. Re-testing with the correct combination resulted in full In the Wild detection and a VB 100% award for the product.