# COMPARATIVE REVIEW

## WINDOWS VISTA X64

*John Hawes*

The final VB100 of the year sees a double whammy of potential pitfalls for our comparative participants – the *Vista* operating system, which still seems shiny and new as well as a little scary (to both developers and users), as well as the x64 architecture, whose ostensible compatibility with standard 32-bit software belies oddities and intricacies that developers ignore at their peril. The announcement of the test brought a few surprises, as several regulars opted to skip this one, but the majority of veteran competitors took part as usual, along with several newer faces, many of whom look set to join the ranks of our regulars.

A total of 25 products were expected to take part, however, due to technical difficulties one of our most reliable participants was unable to provide a product on the deadline date. While some vendors have produced dedicated x64 products, many continue to rely on their standard versions. This was expected to cause some difficulties, and after a setup period considerably shaken by a series of hardware disasters, the legacy of a temperature control failure a few weeks ago which continued to cause problems throughout the testing period, we could only hope to get through this month's test with a modicum of sanity intact.

### PLATFORM AND TEST SETS

Once again we visit the 64-bit edition of *Microsoft*'s *Windows Vista*, which last played host to a VB100 comparative in August 2007. The user base of the *Vista* platform continues to grow slowly, with *XP* still the platform of choice for the vast majority of desktop users – most estimates suggest *XP* resides on between 70% and 80% of systems, while *Vista* still runs on less than 20% almost two years after its introduction. This pattern looks likely to change as sales of *XP* are gradually retired, but hard-core *Vista*-haters continue to insist they'll wait it out and see what the next iteration looks like before abandoning *XP*.

Meanwhile, the x64 architecture, having had a rather longer time to mature, seems to have become the standard for current processors, with straight x86 fading away into the past. The close compatibility between the two, which has helped this growth considerably, means that many continue to use x86 operating systems and not take full advantage of the architecture, while those running full-blown x64 setups expect to find all their 32-bit applications running without difficulty – although, in this area mileage may vary considerably. The AMD64-based hardware used for much of the testing in the *VB* test lab generally idles along happily running 32-bit operating systems, but once in a while we allow it full rein with a platform designed specifically for the architecture. This is always a cause for concern in VB100 testing, where history has taught us that 'fully compatible' doesn't necessarily mean identical behaviours.

The installation and setup of *Vista* is fairly straightforward, but was hampered as usual by the Machiavellian activation process and complications porting images from one system to another for maximum similarity. The standard set of tweaks were made to the default installation after applying the recent service pack – drivers for display and networking hardware were added, network shares connected, and users and passwords set up. For the purposes of this test, an admin-level user was used throughout, with the User Access Controls running in their default state – while we anticipated some annoyances from the likely large numbers of pop-ups, it seemed appropriate to monitor how various products integrated with this safety measure.

The test sets meanwhile underwent their usual minor upgrades, with much of our efforts concentrated on broader upgrades across the lab in preparation for more significant changes in upcoming tests. A sizeable chunk of new software was added to the clean set, and the trojan set used in the previous test was retired and replaced entirely with samples gathered in the last three months. We hope to introduce the same pattern of replenishment with fresh samples for the other test sets in time for the next review, along with some entirely new sets, more on which later.

The WildList set was aligned with the September issue of the WildList, which was released towards the end of October, a few weeks prior to the product deadline. The changes since the previous set included the addition of another flood of online gaming password-stealers, and the retirement of large swathes of older material. These included most of the bot families that once dominated, along with significant numbers of worms such as W32/Stration (aka Warezov) and W32/Rontokbro (aka Brontok). Several more variants of W32/Virut also fell from the list, indicating a gradual decline in numbers of a family which has caused more than its fair share of difficulties in detection, but we hope to add some of these variants to the polymorphic set, in greatly increased numbers, to ensure detection for this tricky kind of malware remains up to scratch. A few other, less sophisticated items were added to this set this month.

With minimal changes to our own sets, and expansion of the WildList set sizeable but fairly uniform, there looked to be few potholes for products to trip on this month.

## Agnitum Outpost Security Suite Pro 2009 6.5.2358.316.0607

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 80.15% |
| **ItW (o/a)** | 100.00% | **Trojans** | 53.04% |
| **Worms & bots** | 99.94% | **False positives** | 0 |


*Agnitum* has become a regular participant in our tests over the past year or so, and the product has made itself welcome with good design and solid functionality. The installation process sparked a yellow alert from the UAC system, defaulting to cancel, followed by some more warnings which were eliminated by allowing the system to 'always trust' *Agnitum*. With these hurdles bypassed, the installation process took a few minutes followed by a reboot, and we were good to go. The interface is simple and clear, with ample controls and fine-tuning available, and everything seemed to run smoothly with no jerks or lags.

Speeds weren't the best, but false positives were absent across the clean and speed sets. Detection in the WildList set was above reproach, and fairly good elsewhere, although a little less than might be hoped for in the trojans set. The product features a variety of behavioural protection mechanisms as part of its main component (the highly regarded firewall), so many of the samples missed in the other sets may in fact be protected against in other ways in a real-world setting. Achieving the VB100 requirements without difficulty, *Agnitum* takes the first award of the month.

## AhnLab V3 Internet Security 7.0 Platinum Edition 7.6.4.1

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 99.78% |
| **ItW (o/a)** | 100.00% | **Trojans** | 66.73% |
| **Worms & bots** | 98.87% | **False positives** | 0 |


*AhnLab*'s product only produced a basic alert from the UAC system, and installed rapidly without the need for a reboot. The interface seemed fairly clear and lucid, but this proved to be deceptive, as numerous vital controls are tucked away where you would least expect them. There were some ominous lags when opening logs (perhaps understandably as large amounts of information were involved) but also when accessing the file system browser as part of the manual scan process. When faced with a 25s pause for a simple browse dialog on a fast modern machine, one could be forgiven for suspecting something is wrong.

Scanning speeds reflected this slightly lethargic attitude, but were far from dismal. Detection rates were much better than expected, after the developers have put some hard work into catching up with the polymorphic set in recent months. Across the clean sets, a large number of files were flagged on demand, which seemed particularly odd as many of them were in areas reserved for files accompanying standard *Windows* installations. Closer inspection of logs showed that the 'malware' in question was labelled 'W97M/Macro', together with the information that a macro removal tool could be used to remove the offending items. After much consideration and close analysis of the wording of logs, it was decided that, though it was a very close call and some users could be alarmed by it, this intentional detection did not count as a full false alarm. *AhnLab* thus qualifies for a VB100 award.

## Alwil avast! 4.8 Pro

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 91.38% |
| **ItW (o/a)** | 100.00% | **Trojans** | 93.21% |
| **Worms & bots** | 99.82% | **False positives** | 1 |

*Alwil*'s *avast!* continues to delight and baffle in equal measure, with a lightning-fast install hindered only by the UAC at the start, followed by a reboot and further UAC pop-ups requesting permission to access the interface. This itself remains unchanged, a combination of stylized simple controls with an 'enhanced' version for power users. The full control system is a rather ungainly thing which, with the benefit of considerable experience, was eventually wrangled into the required shape and lumbered its way through the tests. On-demand scanning speeds were quite impressive, but on-access speeds somewhat less so.

Detection, on the other hand, was superb, with an excellent score in the new trojans set and even better elsewhere. The WildList presented no difficulties, and in the clean sets a number of files in deep archives were warned against as potential decompression bombs. While these caused no problems, another file was mislabelled as malware which, unfortunately for *Alwil*, was enough to spoil its chances of a VB100 this month.

## AVG Internet Security 8.0.199

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 91.74% |
| **ItW (o/a)** | 100.00% | **Trojans** | 96.10% |
| **Worms & bots** | 99.96% | **False positives** | 0 |

*AVG* is a big player in the free-AV market, soon to be joined by an offering from *Microsoft*, but the company's full suite offers an impressive selection of extras. These are made

| On-access detection | WildList viruses | | Worms & bots | | Polymorphic viruses | | Trojans | | Clean sets | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | Missed | % | Missed | % | FP | Susp. |
| Agnitum Outpost | 0 | 100.00% | 2 | 99.94% | 366 | 80.15% | 1213 | 52.69% | | |
| AhnLab V3 Internet Security | 0 | 100.00% | 3 | 99.87% | 51 | 99.78% | 853 | 66.73% | | |
| Alwil avast! | 0 | 100.00% | 3 | 99.82% | 312 | 91.38% | 172 | 93.21% | 1 | |
| AVG Internet Security | 0 | 100.00% | 1 | 99.96% | 52 | 91.74% | 155 | 93.95% | | |
| Avira AntiVir | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 55 | 97.85% | | |
| CA eTrust | 0 | 100.00% | 0 | 100.00% | 177 | 92.51% | 1415 | 44.81% | | |
| ESET NOD32 | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 327 | 87.25% | | |
| Fortinet FortiClient | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1802 | 29.72% | | |
| FRISK F-Prot | 0 | 100.00% | 0 | 100.00% | 121 | 96.46% | 820 | 68.02% | | |
| F-Secure Client Security | 0 | 100.00% | 0 | 100.00% | 60 | 98.24% | 287 | 88.81% | | |
| Kaspersky Anti-Virus | 0 | 100.00% | 0 | 100.00% | 60 | 98.24% | 333 | 87.01% | | |
| Kingsoft Internet Security | 0 | 100.00% | 16 | 99.27% | 1686 | 34.24% | 2068 | 47.39% | | |
| McAfee VirusScan | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 475 | 81.47% | | |
| Microsoft Forefront | 0 | 100.00% | 0 | 100.00% | 130 | 96.04% | 566 | 77.93% | | |
| Microsoft OneCare | 0 | 100.00% | 0 | 100.00% | 130 | 96.04% | 553 | 78.43% | | |
| Norman Virus Control | 0 | 100.00% | 0 | 100.00% | 1079 | 71.06% | 970 | 62.17% | | |
| Quick Heal AntiVirus | 0 | 100.00% | 51 | 95.53% | 986 | 81.31% | 1483 | 42.16% | | |
| Rising Antivirus | 0 | 100.00% | 5 | 99.62% | 1402 | 57.22% | 1632 | 36.35% | | |
| Sophos Anti-Virus | 0 | 100.00% | 0 | 100.00% | 158 | 93.34% | 772 | 69.89% | | 4 |
| Symantec Endpoint Protection | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 765 | 70.16% | | |
| VirusBuster Professional | 0 | 100.00% | 2 | 99.94% | 390 | 78.21% | 1215 | 52.61% | | |
| Webroot I.S. Essentials | 0 | 100.00% | 0 | 100.00% | 813 | 89.83% | 806 | 68.56% | | 2 |

the most of by a main interface crammed to bursting with buttons advertising the various protective layers available, rendering it somewhat cluttered and overwhelming. The installation is quite a slog, with an initial UAC prompt followed by numerous stages including the offer of *Yahoo! Search* toolbars, the setting up of various scheduled checks, selection of networking options and so on, before a reboot finally finishes things off.


Once up and running, the busy interface fairly sensibly requires UAC confirmation to get to the on-access controls, and is reasonably well laid out with accessible but less than comprehensive configuration controls. Speeds were very good on access but a little less splendid on demand where things were a little more thorough. False positives were absent, and detection rates again quite excellent across all sets. With no problems in the WildList, *AVG* wins a VB100 award this month.

## Avira AntiVir Pro 8.2.0.609

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 98.71% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*Avira* is another of the leading players in the free market, if it can be called such, and has an excellent reputation for detection. The product's installation process was a little less slick, with another of the yellow UAC pop-ups warning of 'unidentified' software, and a readme appearing over the

| On demand detection | WildList viruses | | Worms & bots | | Polymorphic viruses | | Trojans | | Clean sets | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Missed | % | Missed | % | Missed | % | Missed | % | FP | Susp. |
| Agnitum Outpost | 0 | 100.00% | 2 | 99.94% | 366 | 80.15% | 1204 | 53.04% | | 3 |
| AhnLab V3 Internet Security | 0 | 100.00% | 3 | 99.87% | 51 | 99.78% | 853 | 66.73% | | 86 |
| Alwil avast! | 0 | 100.00% | 3 | 99.82% | 312 | 91.38% | 172 | 93.21% | 1 | 21 |
| AVG Internet Security | 0 | 100.00% | 1 | 99.96% | 52 | 91.74% | 100 | 96.10% | | |
| Avira AntiVir | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 33 | 98.71% | | |
| CA eTrust | 0 | 100.00% | 0 | 100.00% | 177 | 92.51% | 1273 | 50.35% | | |
| ESET NOD32 | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 227 | 91.15% | | |
| Fortinet FortiClient | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 1802 | 29.72% | | |
| FRISK F-Prot | 0 | 100.00% | 0 | 100.00% | 121 | 96.46% | 769 | 70.01% | | |
| F-Secure Client Security | 0 | 100.00% | 0 | 100.00% | 60 | 98.24% | 279 | 89.12% | | |
| Kaspersky Anti-Virus | 0 | 100.00% | 0 | 100.00% | 60 | 98.24% | 195 | 92.39% | | |
| Kingsoft Internet Security | 0 | 100.00% | 16 | 99.27% | 1668 | 34.95% | 2068 | 47.39% | | |
| McAfee VirusScan | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 448 | 82.53% | | |
| Microsoft Forefront | 0 | 100.00% | 0 | 100.00% | 130 | 96.04% | 381 | 85.14% | | |
| Microsoft OneCare | 0 | 100.00% | 0 | 100.00% | 130 | 96.04% | 483 | 81.16% | | |
| Norman Virus Control | 0 | 100.00% | 0 | 100.00% | 768 | 81.03% | 932 | 63.65% | 1 | |
| Quick Heal AntiVirus | 0 | 100.00% | 48 | 95.79% | 986 | 81.31% | 1114 | 56.55% | | |
| Rising Antivirus | 0 | 100.00% | 3 | 99.80% | 1332 | 60.80% | 1180 | 53.98% | | |
| Sophos Anti-Virus | 0 | 100.00% | 0 | 100.00% | 158 | 93.34% | 734 | 71.37% | | 6 |
| Symantec Endpoint Protection | 0 | 100.00% | 0 | 100.00% | 0 | 100.00% | 753 | 70.63% | | |
| VirusBuster Professional | 0 | 100.00% | 2 | 99.94% | 390 | 78.21% | 1201 | 53.16% | | |
| Webroot I.S. Essentials | 0 | 100.00% | 0 | 100.00% | 813 | 89.83% | 799 | 68.84% | | 2 |

top of a dialog box towards the end. The installation was followed by an attempt to scan the system, which was eventually stopped after some initial difficulties, and testing got under way.


The interface is another of those that appears straightforward but has deceptive moments of illogic, and this was not only apparent on the surface. Several attempts to run scans were found to be failing to access files, an oddity eventually diagnosed as being caused by the on-access scanner preventing the on-demand scanner from working properly. With the appropriate parts disabled, all tests were run through at their usual superb speed and with incredible accuracy. With barely anything missed and not a shadow of a false alarm, *Avira* justly earns a VB100 award for its product's performance.

## CA eTrust 8.1.637.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 92.51% |
| **ItW (o/a)** | 100.00% | **Trojans** | 50.35% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*CA*'s product has remained unchanged over several VB100 tests, with the same main installer used each time and simple updates provided for each test. The lengthy installation process with its multiple EULAs runs through on automatic, after an initial

UAC prompt, and was only enlivened this time by a failing updater – an error was diagnosed thanks to the 'x86' in the file's name, rather than from the rather misleading error message, and with a 64-bit version duly replacing it things moved along.

The interface is something of a horror – this time it was less sluggish to respond than usual, but still awkward and fiddly, with access to logging data almost impossible. Some of the functions continue to bemuse, such as the engine selection button which continues to hang around years after the product's optional second engine was dropped, and the conspicuous lack of archive scanning on access despite clear options to enable it. Nevertheless, scanning speeds remain lightning-fast, and detection rates decent, although a little poor on the trojans set. With no false positives and no items missed in the WildList set, *CA* earns yet another VB100 award.

## ESET NOD32 Antivirus 3.0.672.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 91.15% |
| **Worms & bots** | 100.00% | **False positives** | 0 |


The latest iteration of *ESET*'s product started with another fairly straightforward install, despite dragging on somewhat during the file-copying phase and with a UAC prompt halfway through. It retains its stylish good looks and decent navigability, along with speeds which seem slightly less impressive than in previous versions but still well ahead of the crowd. Some sensible defaults and comprehensive options made for easy testing. The performance was marred by a few buggy moments, the occasional refusal to cooperate and on a couple of occasions full-on freezes, requiring a reboot to regain access to the controls. There were also a few occasions where options appeared to respond in ways not entirely expected.

All this did little to dent an otherwise solid performance, and detection rates were solid with high marks across the board. No trouble with the WildList samples and no false positives means that yet another VB100 award is earned by *ESET*.

## Fortinet FortiClient 3.0.606

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 29.72% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*FortiClient* brought up another of the yellow UAC prompts during its installation, and some scarier red ones as various driver components were installed. Once the reboot was completed some more confirmation requests were presented when going through the setup process and accessing configuration. Some extremely thorough defaults meant little of this was required, but slowed down the speed tests somewhat. Nevertheless, respectable scanning speeds were evident.


Detection rates were mostly excellent, although in the trojans set the rate dropped sharply; liaison with the developers after a similar performance in the last test suggested many of the items included in the set are covered by the product's greyware detections, not enabled by default. However, a rescan with these settings turned on produced few extra detections.

Despite this, the WildList was covered just fine, and without false positives *Fortinet* also wins a VB100 award.

## FRISK F-Prot 6.0.9.1

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 96.46% |
| **ItW (o/a)** | 100.00% | **Trojans** | 70.01% |
| **Worms & bots** | 100.00% | **False positives** | 0 |


*F-Prot* is a much simpler beast than the suites and multi-tools proffered by many other participants in our tests these days, and as such its installation and use is expected to be less strenuous. The pared-down, wintry interface offers little in the way of user control or interactivity, but goes about its business in a workman-like way. Accessing logs, somewhat unexpectedly, required acceptance of a UAC pop-up, but little else hindered testing as we tripped merrily through the speed tests and ploughed through the infected sets with splendid detection and a lack of false positives. Full coverage of the WildList grants *FRISK* another VB100 award for its tally.

## F-Secure Client Security 8.00 build 232

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 98.24% |
| **ItW (o/a)** | 100.00% | **Trojans** | 89.12% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*F-Secure* returns us to the more complex world of multi-layer protection, the product including the company's new and much-vaunted *Deepguard* system, using an online reputation database in addition to local information as part of the behavioural protection system. Sadly, the impact of this could not be fully analysed in our current test setup, but

| | | ACE | CAB | JAR | LZH | RAR | TGZ | ZIP | ZIP-SFX | EXT* |
|---|---|---|---|---|---|---|---|---|---|---|
| Agnitum Outpost | OD | 2 | √ | √ | X | √ | √ | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | √ |
| AhnLab V3 Internet Security | OD | X | 9 | X | 9 | 9 | X | 9 | X | √ |
| | OA | X | X | X | X | X | X | X | X | √ |
| Alwil avast! | OD | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| | OA | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | √ | √ |
| AVG Internet Security | OD | X | √ | X | X | √ | X | √ | √ | X/√ |
| | OA | X | X | X | X | X | X | X | X | √ |
| Avira AntiVir | OD | √ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| | OA | X | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| CA eTrust | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | 1 | X | X | X | 1 | X | √ |
| ESET NOD32 | OD | X | √ | X | √ | √ | 5 | √ | √ | √ |
| | OA | X | X | X | X | X | X | X | X | √ |
| Fortinet FortiClient | OD | X | √ | √ | √ | √ | √ | √ | 4 | √ |
| | OA | X | √ | √ | √ | √ | √ | √ | 4 | √ |
| FRISK F-Prot | OD | 1 | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | 1 | X | 2 | 2 | X | X | X | 2 | √ |
| F-Secure Client Security | OD | X/√ | 5 | 5 | 5 | 5 | 2 | 5 | 5 | √ |
| | OA | X/√ | X/5 | X/5 | X/5 | X/5 | X/2 | X/5 | X/5 | X/√ |
| Kaspersky Anti-Virus | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/4 | X/4 | X/4 | X/4 | X/5 | X/1 | X/2 | X/1 | X/√ |
| Kingsoft Internet Security | OD | X | X | √ | √ | √ | √ | √ | X | √ |
| | OA | X | X | X | X | X | X | X | X | √ |
| McAfee VirusScan | OD | 2 | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X/2 | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ | X/√ |
| Microsoft Forefront | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | X | X | 1 | X | X | X | 1 | 1 | √ |
| Microsoft OneCare | OD | X | X | 1 | X | X | X | 1 | 1 | √ |
| | OA | X | X | 1 | X | X | X | 1 | 1 | √ |
| Norman Virus Control | OD | X | X | √ | √ | √ | √ | √ | X | √ |
| | OA | X | X | X | X | X | X | X | X | √ |
| Quick Heal AntiVirus | OD | X/2 | X/5 | 2/5 | X | 2/5 | X/1 | 2/5 | X | X/√ |
| | OA | X | X | X | X | X | X | X | X | X |
| Rising Antivirus | OD | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| | OA | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Sophos Anti-Virus | OD | X | 5 | 5 | 5 | 5 | 5 | 5 | 5 | √ |
| | OA | X | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | X/5 | √ |
| Symantec Endpoint Protection | OD | X | 3/√ | 3/√ | 3/√ | 3/√ | 3/√ | 3/√ | 3/√ | √ |
| | OA | X | X | X | X | X | X | X | X/√ | √ |
| VirusBuster Professional | OD | √ | √ | X | X | √ | √ | √ | √ | X |
| | OA | X | X | X | X | X | X | X | X | X |
| Webroot I.S. Essentials | OD | X | √ | 5 | √ | √ | 5 | √ | 5 | √ |
| | OA | X | X | X | X | X | X | X | X | √ |

Key:
X - Archive not scanned
√ - Archives scanned to depth of 10 or more levels
[1-9] - Archives scanned to limited depth
X/√ - Default settings/thorough settings
*Executable file with randomly chosen extension


the rest of the product seemed pretty solid for the most part.

The installer runs through nice and simply, with a UAC prompt at the start and the selection of local or remote management the only non-standard moments. Once installed, and after a reboot, testing proceeded fairly slowly, thanks to the in-depth multi-engine approach, and the only blot on the performance was a loss of connectivity between various parts of the product at one stage – attempts to set off an on-demand scan were met with messages telling us the 'AV handler' was not running. Another reboot soon fixed this, and the problem did not recur. We powered through

| On-demand throughput (MB/s) | Archive files | | | | Binaries and system files | | | | Media and documents | | | | Other file types | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Default settings | | All files | | Default settings | | All files | | Default settings | | All files | | Default settings | | All files | |
| | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) | Time (s) | Through-put (MB/s) |
| Agnitum Outpost | 942 | 3.24 | 942 | 3.24 | 339 | 7.66 | 339 | 7.66 | 143 | 14.43 | 143 | 14.43 | 94 | 10.02 | 94 | 10.02 |
| AhnLab V3 Internet Security | 1683 | 1.82 | 1683 | 1.82 | 394 | 6.59 | 394 | 6.59 | 185 | 11.16 | 185 | 11.16 | 210 | 4.49 | 210 | 4.49 |
| Alwil avast! | 34 | 89.86 | 612 | 4.99 | 191 | 13.60 | 219 | 11.86 | 56 | 36.86 | 94 | 21.96 | 207 | 4.55 | 231 | 4.08 |
| AVG Internet Security | 1253 | 2.44 | 1253 | 2.44 | 267 | 9.73 | 267 | 9.73 | 273 | 7.56 | 273 | 7.56 | 40 | 23.56 | 144 | 6.54 |
| Avira AntiVir | 265 | 11.53 | 289 | 10.57 | 93 | 27.93 | 88 | 29.52 | 53 | 38.94 | 49 | 42.12 | 32 | 29.45 | 42 | 22.43 |
| CA eTrust | 264 | 11.57 | 264 | 11.57 | 157 | 16.54 | 157 | 16.54 | 68 | 30.35 | 68 | 30.35 | 36 | 26.17 | 36 | 26.17 |
| ESET NOD32 | 756 | 4.04 | 756 | 4.04 | 367 | 7.08 | 367 | 7.08 | 40 | 51.60 | 40 | 51.60 | 82 | 11.49 | 82 | 11.49 |
| Fortinet FortiClient | 286 | 10.68 | 286 | 10.68 | 377 | 6.89 | 377 | 6.89 | 40 | 51.60 | 40 | 51.60 | 90 | 10.47 | 90 | 10.47 |
| FRISK F-Prot | 293 | 10.43 | 293 | 10.43 | 341 | 7.62 | 341 | 7.62 | 51 | 40.47 | 51 | 40.47 | 41 | 22.98 | 41 | 22.98 |
| F-Secure Client Security | 1397 | 2.19 | 1852 | 1.65 | 301 | 8.63 | 296 | 8.77 | 66 | 31.27 | 167 | 12.36 | 40 | 23.56 | 133 | 7.08 |
| Kaspersky Anti-Virus | 591 | 5.17 | 591 | 5.17 | 137 | 18.96 | 137 | 18.96 | 53 | 38.94 | 53 | 38.94 | 37 | 25.47 | 37 | 25.47 |
| Kingsoft Internet Security | 6945 | 0.44 | 6945 | 0.44 | 1311 | 1.98 | 1311 | 1.98 | 619 | 3.33 | 619 | 3.33 | 1166 | 0.81 | 1166 | 0.81 |
| McAfee VirusScan | 700 | 4.36 | 700 | 4.36 | 321 | 8.09 | 321 | 8.09 | 83 | 24.87 | 83 | 24.87 | 112 | 8.41 | 112 | 8.41 |
| Microsoft Forefront | 841 | 3.63 | 841 | 3.63 | 860 | 3.02 | 860 | 3.02 | 69 | 29.91 | 69 | 29.91 | 95 | 9.92 | 95 | 9.92 |
| Microsoft OneCare | 1034 | 2.95 | NA | NA | 495 | 5.25 | 495 | 5.25 | 88 | 23.45 | 88 | 23.45 | 71 | 13.27 | 71 | 13.27 |
| Norman Virus Control | 618 | 4.94 | 618 | 4.94 | 1332 | 1.95 | 1332 | 1.95 | 99 | 20.85 | 99 | 20.85 | 218 | 4.32 | 218 | 4.32 |
| Quick Heal AntiVirus | 300 | 10.18 | 596 | 5.13 | 64 | 40.58 | 67 | 38.77 | 79 | 26.13 | 90 | 22.93 | 50 | 18.85 | 63 | 14.96 |
| Rising Antivirus | 1391 | 2.20 | 1391 | 2.20 | 665 | 3.91 | 665 | 3.91 | 254 | 8.13 | 254 | 8.13 | 215 | 4.38 | 215 | 4.38 |
| Sophos Anti-Virus | 336 | 9.09 | 336 | 9.09 | 223 | 11.65 | 223 | 11.65 | 89 | 23.19 | 89 | 23.19 | 91 | 10.35 | 91 | 10.35 |
| Symantec Endpoint Protection | 430 | 7.10 | 452 | 6.76 | 168 | 15.46 | 243 | 10.69 | 117 | 17.64 | 175 | 11.79 | 97 | 9.71 | 99 | 9.52 |
| VirusBuster Professional | 462 | 6.61 | 2645 | 1.16 | 190 | 13.67 | 1753 | 1.48 | 37 | 55.78 | 316 | 6.53 | 21 | 44.87 | 170 | 5.54 |
| Webroot I.S. Essentials | 738 | 4.14 | 738 | 4.14 | 270 | 9.62 | 270 | 9.62 | 107 | 19.29 | 107 | 19.29 | 115 | 8.19 | 155 | 6.08 |

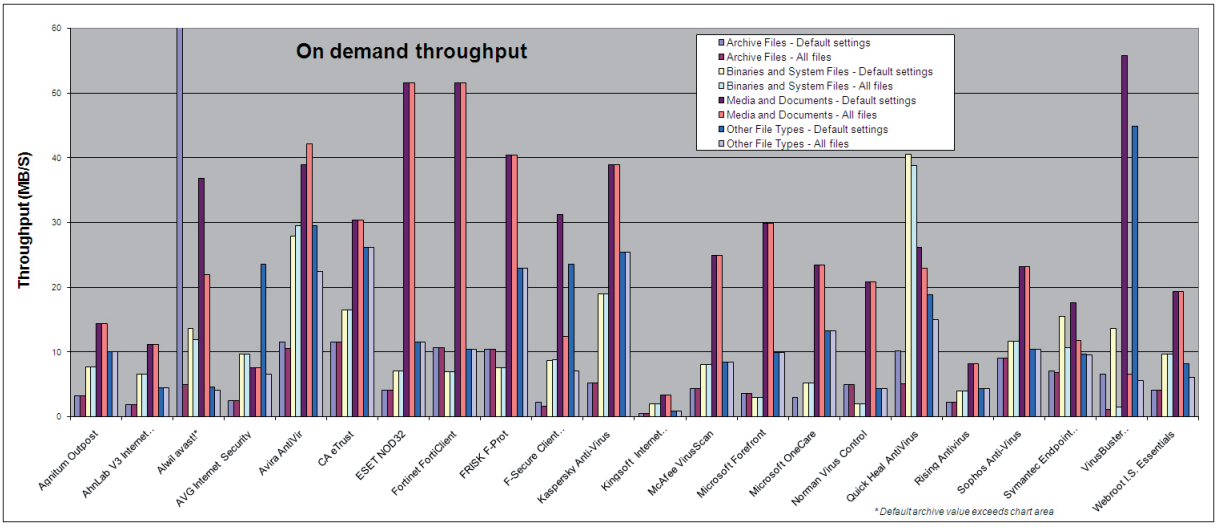
the infected sets with excellent detection rates, scored no false positives in the clean sets and covered the WildList flawlessly. Another VB100 goes to *F-Secure* for the product's performance.

## Kaspersky Anti-Virus 2009 8.0.0.454

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 98.24% |
| **ItW (o/a)** | 100.00% | **Trojans** | 92.39% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*Kaspersky*'s latest offering provoked considerable enthusiasm from our test engineer, who was impressed by the wide range of protective layers provided as well as the pleasant and informative interface with its range of data displays, including rolling graphs of monitored files and blocked attacks.

Glancing over the test results, scanning speeds were similarly impressive, and detection rates at their usual high level.




With the full range of VB100 requirements met without difficulty, *Kaspersky* also makes the grade and wins the award.

## Kingsoft Internet Security 2008.11.6.63

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 34.95% |
| **ItW (o/a)** | 100.00% | **Trojans** | 47.39% |
| **Worms & bots** | 99.27% | **False positives** | 0 |

*Kingsoft* has been on a bit of a rollercoaster of late, with various product and detection issues meaning its record of VB100s has been somewhat sporadic. This time, however, the product seemed to behave itself for the most part.

After a rather lengthy but mostly quite straightforward installation process, testing ran along mainly using the default settings, as in-depth configuration was limited. No signs of the product's previous instability issues were evident. The only problem encountered was in accessing the logs, as the various buttons to access the 'log viewer' system appeared disabled. After some poking around we found that this was another UAC problem, silent this time, and the logs could be accessed by running the viewer with admin rights from the start menu.

Speeds were remarkable, although not for the happiest of reasons, and detection rates left much to be desired in several sets. However, the WildList samples all detected correctly and no files were falsely alerted on in the clean test set, which means that *Kingsoft* makes the grade for another VB100 award.

## McAfee VirusScan Enterprise 8.7.0i

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 82.53% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

A quite different kettle of fish, *McAfee*'s product is a veteran war horse which has weathered many VB100s with barely a stumble. The product remains little changed, presenting a plain and unfussy face to the world but providing all the fine-tuning options expected of an enterprise-level product beneath its bonnet.

Our test engineer felt *VirusScan* was rather more affected by UAC blocks than some other products, and the system took considerably longer than usual to regain its desktop after the post-install reboot, but otherwise no issues were observed, with good scanning speeds and very good detection rates. No problems in the WildList or clean sets means that *McAfee* qualifies comfortably for another VB100 award.

## Microsoft Forefront Client Security 1.5.1955.0

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 96.04% |
| **ItW (o/a)** | 100.00% | **Trojans** | 85.14% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*Microsoft*'s corporate product offers considerably fewer of those fine-tuning options than the product discussed above, at least at the desktop level, presenting an interface described by our test engineer as 'very simple', with not many options but lots of help. The absence of in-depth

| File access lag time (s/MB) | Archive files | | | | Binaries and system files | | | | Media and documents | | | | Other file types | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Default settings | | All files | | Default settings | | All files | | Default settings | | All files | | Default settings | | All files | |
| | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) | Time (s) | Lag (s/MB) |
| Agnitum Outpost | 61 | 0.019 | NA | NA | 265 | 0.096 | 265 | 0.096 | 178 | 0.071 | 178 | 0.071 | 143 | 0.128 | 143 | 0.128 |
| AhnLab V3 Internet Security | 79 | 0.025 | NA | NA | 220 | 0.078 | 220 | 0.078 | 120 | 0.043 | 120 | 0.043 | 144 | 0.129 | 144 | 0.129 |
| Alwil avast! | 143 | 0.046 | 684 | 0.223 | 457 | 0.170 | 275 | 0.100 | 159 | 0.062 | 198 | 0.081 | 147 | 0.132 | 154 | 0.140 |
| AVG Internet Security | 151 | 0.048 | 174 | 0.056 | 345 | 0.127 | 379 | 0.140 | 127 | 0.046 | 170 | 0.067 | 40 | 0.019 | 117 | 0.101 |
| Avira AntiVir | 35 | 0.010 | 291 | 0.094 | 102 | 0.033 | 109 | 0.036 | 66 | 0.017 | 86 | 0.027 | 33 | 0.012 | 61 | 0.041 |
| CA eTrust | 26 | 0.007 | NA | NA | 76 | 0.023 | 76 | 0.023 | 75 | 0.022 | 75 | 0.022 | 51 | 0.031 | 51 | 0.031 |
| ESET NOD32 | 12 | 0.003 | NA | NA | 52 | 0.014 | 52 | 0.014 | 78 | 0.023 | 78 | 0.023 | 95 | 0.077 | 95 | 0.077 |
| Fortinet FortiClient | 276 | 0.089 | 276 | 0.089 | 367 | 0.135 | 367 | 0.135 | 68 | 0.018 | 68 | 0.018 | 123 | 0.108 | 123 | 0.108 |
| FRISK F-Prot | 72 | 0.023 | NA | NA | 396 | 0.146 | 396 | 0.146 | 64 | 0.016 | 64 | 0.016 | 51 | 0.031 | 51 | 0.031 |
| F-Secure Client Security | 45 | 0.014 | 1682 | 0.549 | 313 | 0.114 | 448 | 0.166 | 108 | 0.037 | 307 | 0.134 | 58 | 0.038 | 201 | 0.190 |
| Kaspersky Anti-Virus | 27 | 0.008 | 104 | 0.033 | 131 | 0.044 | 307 | 0.112 | 105 | 0.036 | 117 | 0.042 | 66 | 0.047 | 92 | 0.075 |
| Kingsoft Internet Security | 84 | 0.026 | NA | NA | 1353 | 0.515 | 1353 | 0.515 | 682 | 0.316 | 682 | 0.316 | 1079 | 1.122 | 1079 | 1.122 |
| McAfee VirusScan | 43 | 0.013 | 462 | 0.150 | 274 | 0.099 | 259 | 0.094 | 112 | 0.040 | 115 | 0.041 | 114 | 0.098 | 117 | 0.101 |
| Microsoft Forefront | 137 | 0.044 | NA | NA | 433 | 0.160 | 433 | 0.160 | 91 | 0.029 | 91 | 0.029 | 115 | 0.099 | 115 | 0.099 |
| Microsoft OneCare | 147 | 0.047 | NA | NA | 487 | 0.181 | 487 | 0.181 | 113 | 0.040 | 113 | 0.040 | 82 | 0.063 | 82 | 0.063 |
| Norman Virus Control | 57 | 0.018 | NA | NA | 242 | 0.087 | 242 | 0.087 | 114 | 0.040 | 114 | 0.040 | 188 | 0.177 | 188 | 0.177 |
| Quick Heal AntiVirus | 14 | 0.003 | NA | NA | 76 | 0.023 | NA | NA | 68 | 0.018 | NA | NA | 33 | 0.012 | NA | NA |
| Rising Antivirus | 25 | 0.007 | 25 | 0.007 | 744 | 0.280 | 744 | 0.280 | 281 | 0.121 | 281 | 0.121 | 155 | 0.141 | 155 | 0.141 |
| Sophos Anti-Virus | 39 | 0.012 | 1523 | 0.497 | 217 | 0.077 | 799 | 0.301 | 70 | 0.019 | 143 | 0.055 | 52 | 0.032 | 140 | 0.125 |
| Symantec Endpoint Protection | 29 | 0.008 | NA | NA | 125 | 0.042 | 125 | 0.042 | 75 | 0.021 | 75 | 0.021 | 89 | 0.071 | 89 | 0.071 |
| VirusBuster Professional | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| Webroot I.S. Essentials | 24 | 0.007 | NA | NA | 35 | 0.007 | NA | NA | 42 | 0.005 | NA | NA | 38 | 0.017 | NA | NA |

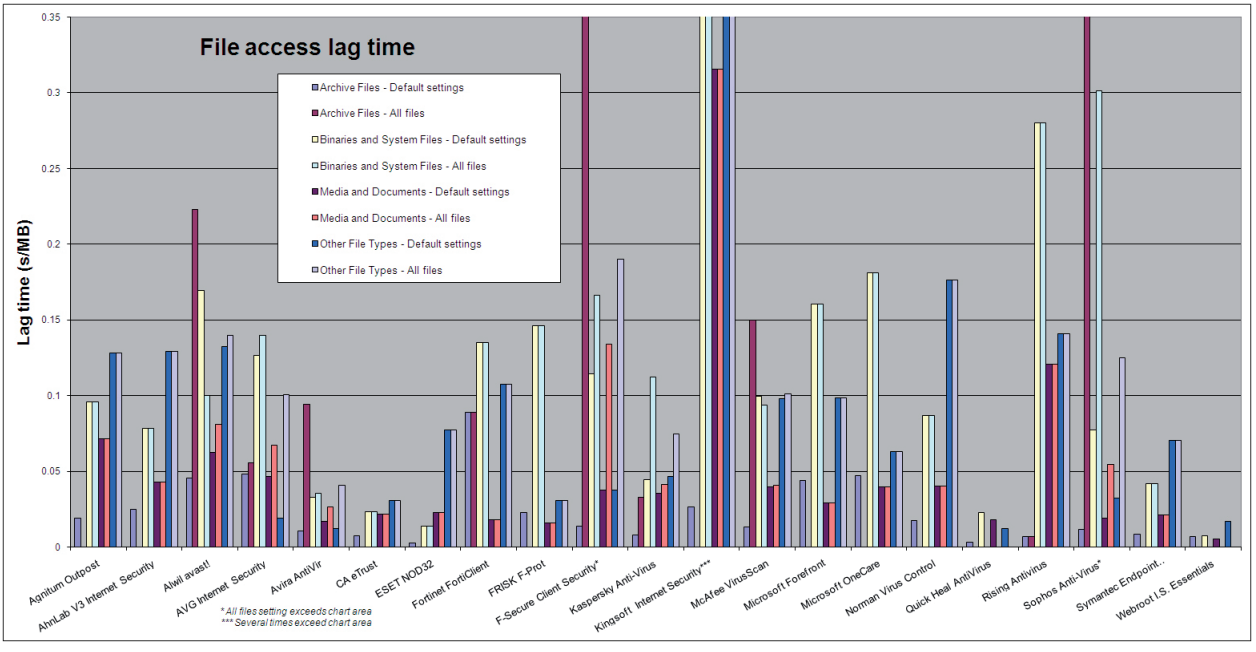
configuration made for fairly straightforward testing, and the defaults seemed generally fairly sensible, with in-depth logging, not previously revealed to us by the developers, finally put to good use and the awkward event log system no longer required. One oddity of the logging was frequent warnings about 'expensive' files, but as there is nothing in the VB100 rules about overestimating the value of software, we let this pass.


The results showed fairly decent scanning speeds and detection rates were once again greatly improved. No false positives, and still no WildList misses, means another VB100 award goes to *Forefront* this month.

## Microsoft OneCare 2.5.2900.15

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 96.04% |
| **ItW (o/a)** | 100.00% | **Trojans** | 81.16% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

Many will have been shaken this month by the news that *OneCare*, *Forefront*'s home-user sibling, is to be retired next year and replaced by a livelier, simpler model. *VB* will not




be mourning too deeply, although we will be looking forward with some interest to the new version.

As it stands, *OneCare* is even simpler than *Forefront*, despite the various extra functions included, such as backup and disk defragmentation. There is very little opportunity for the user to manipulate its behaviour beyond the very basics, and on several occasions we found test systems completely crippled, and scan logs rendered inaccessible, by unexpected runs of 'tune-up' tasks. On most occasions, once this problem was diagnosed and the tasks aborted, a simple reboot allowed access to logs once more, despite the ominous tone of the error messages.

Speed results proved very slightly slower than *Forefront*, and detection rates pretty similar, with an identical lack of difficulties in the WildList and clean set resulting in another VB100 award for *Microsoft*.

## Norman Virus Control 5.99

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 81.03% |
| **ItW (o/a)** | 100.00% | **Trojans** | 63.65% |
| **Worms & bots** | 100.00% | **False positives** | 1 |

*Norman*'s unusual multi-interface approach made for more interference than usual from the UAC pop-ups, as various different parts of the product required individual confirmation. This meant that there were some rather long pauses moving from one part to another in the process of carrying out our various tasks. Configuration was patchy – in-depth in some areas and apparently absent in others, but things got done once the control system had been deciphered.

Scanning speeds were somewhat below average, but detection rates were pretty reasonable in general, with no difficulty covering the WildList. In the clean sets, however, a single file was mislabelled as the notorious Zlob trojan, and this was enough to spoil *Norman*'s chances for a VB100 award this month.

## Quick Heal AntiVirus 9.50

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 81.31% |
| **ItW (o/a)** | 100.00% | **Trojans** | 56.55% |
| **Worms & bots** | 95.79% | **False positives** | 0 |

*Quick Heal* proved once again to be worthy of its name, with testing completed fairly quickly once our test engineer had found his way around the interface. He described the interface as 'bizarrely laid out', and said that it seemed to keep some of its important functions quite well hidden.

Along with the excellent scanning speeds went less-than-superb detection rates, with detection for large numbers of items recently retired from the WildList apparently removed from databases – presumably to maintain that excellent scan rate. The WildList itself, however, was covered without problems, and without false positives *Quick Heal* is worthy of a VB100 award.

## Rising Antivirus 20.67.10

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 60.80% |
| **ItW (o/a)** | 100.00% | **Trojans** | 53.98% |
| **Worms & bots** | 99.80% | **False positives** | 0 |


*Rising* is another relative newcomer to the VB100 award, but the company has done pretty well so far with a nicely designed product. The setup process in this case was fairly complex, with a yellow warning from the UAC system and further configuration requirements after the reboot.

The stability that was noted with approval in previous tests was sadly less evident this time, with some oddities of behaviour and downright crashes slowing down the progress of our testing. On one occasion, after an on-demand scan of clean files, the ominous message 'Rising Antivirus has stopped working' appeared, while several times during on-access testing file accesses seemed to accelerate rapidly, and detections cut off completely, implying that the on-access scanner had also cut out.

After several retries some reasonably reliable results were obtained, showing some rather sluggish scanning speeds and less-than-perfect detection rates, but the WildList at least was well handled, and without false positives *Rising* also qualifies for a VB100 award.

## Sophos Anti-Virus 7.6.1

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 93.34% |
| **ItW (o/a)** | 100.00% | **Trojans** | 71.37% |
| **Worms & bots** | 100.00% | **False positives** | 0 |


*Sophos* is another veteran participant in the VB100, and the product impressed our tester with its speed of installation, well laid out interface and depth of configuration. UAC prompts seemed to accompany most selections from the main part of the interface.

Scanning speeds were pretty fast, at least with the default settings, and detection rates generally decent too, with no problems in the WildList and no false positives. *Sophos* thus joins the ranks of this month's VB100 award winners.

## Symantec Endpoint Protection 11.0.3001.2224

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 100.00% |
| **ItW (o/a)** | 100.00% | **Trojans** | 70.63% |
| **Worms & bots** | 100.00% | **False positives** | 0 |


*Symantec*'s business desktop product has had a serious redesign of late, and the new look and feel has moved sharply away from the business-like, configurable simplicity of the previous edition towards the colourful and over-simplified. Though scanning speeds were decent, there were some very noticeable lags on various button presses, especially when trying to access the logs. These were most likely caused by the raw data, which in the case of our test runs often ran to hundreds of megabytes. Similar lags were also observed after some longer scan jobs.

Nevertheless, detection rates were solid, with no problems in the WildList or in the clean sets, and thus *Symantec* wins another VB100 award too.

## VirusBuster Professional 6.0 build 206

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 78.21% |
| **ItW (o/a)** | 100.00% | **Trojans** | 53.16% |
| **Worms & bots** | 99.94% | **False positives** | 0 |


*VirusBuster*'s installer needed to be run with full admin rights to function, but was still interrupted by the UAC prompts. After this, the installation was fast and simple, all done in less than 30 seconds, but this speed did not extend to the testing, with our tester finding the interface 'appalling'. The convoluted layout, and lack of progress information on scanning times, didn't make *VirusBuster* any new friends in the *VB* lab.

While on-demand scanning times were pretty decent, on-access times could not be gathered, as the product's usual on-read detection appeared not to be functioning as expected on the platform under test. On-access results were thus obtained by copying file sets to the system with the product set to delete, and analysing the remains to measure accuracy. This proved mostly quite decent, with no difficulties in the WildList and no false positives, and *VirusBuster* is thus awarded another VB100 for its efforts.

## Webroot I.S. Essentials 6.0.2.22

| | | | |
|---|---|---|---|
| **ItW** | 100.00% | **Polymorphic** | 89.83% |
| **ItW (o/a)** | 100.00% | **Trojans** | 68.84% |
| **Worms & bots** | 100.00% | **False positives** | 0 |

*Webroot*'s '*WISE*' was another product that failed to impress our tester, with an interface that looked attractive on the surface, but quickly grew ugly when trying to do anything beyond the very basics. Configuration is very minimal, and

responsiveness somehow even lower, with huge time lags between various components, most notably the file browsing to select areas to scan. Scanning times were also rather slow, and although once again the on-access component appeared not to be sparked by simple file accesses, times were still recorded for this test as they were in some cases slower than other products that did scan the files.


Logging also proved an issue, with all data discarded after 1,000 lines, not much by the standards we require. Nevertheless, with a combination of careful scanning of tiny portions of our sets at a time, copying files around and to the system and allowing the product to mangle them as it saw fit, then comparing the results with the originals to check for changes, we finally managed to get some usable results. The results seemed to tally fairly closely with those of the *Sophos* engine at the core of the product's detection capabilities. This meant that there were no issues in either the WildList or clean sets, and that, despite annoying the test team quite thoroughly, *Webroot* earned another VB100 award.

## CONCLUSIONS

On top of the already rather arduous task of getting through multiple tests on multiple products, this month presented more than the average number of small annoyances and petty frustrations. These included bizarre and buggy interfaces, hidden or absent options, and unreliable behaviours, as well as a few more major issues, including product freezes and crashes, blatant contradiction of advertised behaviours, and the occasional product which all but defied testing. Much of this can be put down to the less than ubiquitous platform, but developers claiming to support a given platform need to ensure that their products undergo full and thorough quality assurance.

This month's test has been notable for the more than usually high number of passes – indeed only two products failed to meet the required standard, with a couple of other close calls. It seems appropriate to remind readers that we expect products to pass our base test requirements on a regular basis, that the VB100 requirements are not intended as an indication of superlative products, merely of adequate and reasonably reliable ones. The purpose of the scheme is to provide certification of products proven to be legitimate, and to provide a basic level of protection. A single test result should not be taken in a vacuum, but patterns and trends of performance over time can be a valuable guide to the trustworthiness of a product and its developers.

In addition to the plain pass/fail outcomes which some take to be the be-all and end-all of the VB100, we provide a wide range of additional information on the products that take part, including measurements of scanning speed and overheads, overviews of additional functionality and usability, and detection rates over a selection of additional test sets.

In the next VB100, we plan to introduce a major addition to this range of extras, based on weekly test sets built up in the weeks immediately prior to, and shortly after, the product submission deadline. This should provide a useful indicator of how well developers are keeping up with the ever-growing flood of new malware samples seen on a daily basis, many of them frequently morphed and fine-tuned with the explicit aim of avoiding detection by anti-malware software. The test should also provide some insight into how well heuristic and generic detection techniques are allowing products to detect malware as yet unseen by analysis labs.

Details of the new test system, which we have dubbed '*RAP*', standing for *Reactive And Proactive* measuring, were presented at the recent *VB* conference and have since been opened to deeper consultation with interested parties. In its fully developed form the new test should provide clear and easily understood additional data, which will also build up over time to show long-term trends and patterns of improvement, stagnation or decline in the performance of scanner products.

This will go some way to providing more information on the performance and capabilities of current security software, but of course there are many diverse new functions being added to solutions with every new generation, many of which require major shifts in test design to properly measure their efficacy. In conjunction with groups like AMTSO, our own expert advisory board and other interested parties, we will continue to investigate and develop new testing methodologies, and even new certification schemes, that will enable us to more accurately evaluate the products' full capabilities. We hope to make many more strides in this direction in the course of the coming year, and as always we welcome any feedback, input, suggestions and opinions from our readers.

**Technical details**

All products were tested on identical systems with *AMD Athlon64 X2* Dual Core 5200+ processors, 2 GB RAM, dual 80 GB and 400 GB hard drives, running *Microsoft Windows Vista Business Edition* (64-bit).

*Developers interested in submitting products for Virus Bulletin's comparative reviews should contact john.hawes@virusbtn.com. A schedule of forthcoming tests can be found at http://www.virusbtn.com/vb100/about/schedule.xml.*

## ADDENDUM: VB100 COMPARATIVE REVIEW

*VB* regrets that, due to an oversight, the *MicroWorld Technologies eScan* product was omitted from the write-up of the VB100 comparative review on *Windows Vista x64* (see *VB*, December 2008, p.14). In fact, *eScan* detected all of the samples in the WildList test set and did not generate any false positives when scanning the clean test set – thus the product qualifies for a VB100 award. *VB* extends its apologies to *MicroWorld* for the omission.