

VB100 – WINDOWS SERVER 2008 R2

Following our usual pattern of alternating between desktop and server platforms, we come this month to *Microsoft's* latest upgrade to its server solution. This is presented as a simple refresh of the 2008 version, but in fact is a much bigger deal, essentially being *Windows 7 Server*. The new platform is considerably revised and updated, and is available only for 64-bit hardware. We expected that this combination of a new platform and the use of full x64 would deter some vendors from entering products for what could be a rather tricky test, but in fact we were inundated with far more entries than we had anticipated. With the working month shortened by some urgent lab maintenance and a cluster of conferences, it looked like the lab team would once again be getting little rest as we hurried along, hoping as usual for well-behaved and reliable products to deal with.

PLATFORM AND TEST SETS

Installation of the test systems was a fairly simple process, with the set-up process for the new platform closely mirroring that of *Windows 7* and running smoothly on our shiny new batch of test systems. These were all fully supported from the off with no need for additional drivers etc. Having made a few standard adjustments, installed some useful software such as PDF viewers in case any help files might need perusal, and configured networking to fit in with our lab set-up, we were ready to take snapshots and move on to preparing the test sets. The most interesting aspect of the platform preparation process was the requirement for a small additional partition on the hard drive. Small adjustments to our reimaging set-up were required to ensure both partitions were reset to their original status for each test run.

Test set preparation was a rather more arduous task, with much work required to bring the lab systems back up to full functionality after having been neglected during the hectic period of the last comparative. With space running out and more processing power required, a few hasty temporary fixes were required to enable us make a start on this month's test.

The core WildList test set saw a sprinkling of new additions, with an early test deadline meaning we just missed the release of the March list; the sets were instead aligned with the February list, which included the same W32/Virut strain that caused some upsets last time around, as well as the venerable W32/Polip which was generally handled more solidly. New additions followed the trend of recent months, dominated by W32/Koobface worms with little else of particular novelty or interest.

The other core part of the certification set, the clean sample set, saw some considerable expansion, with the usual addition of the most popular items from various freeware sites supplemented with swathes of more serious software packages from *Microsoft*, *Sun* and others as a nod to the server setting of this month's test.

The remaining sets followed the usual pattern. A small adjustment to the polymorphic set was made to increase the representation of some of the more recent and prevalent items, while some older and less interesting families were retired from the set. The trojans and worms & bots sets were built with samples gathered in the period between the last test and the start of this month's RAP period. The RAP samples were sorted into their weekly sets, which were somewhat larger than previous ones thanks to increased sample-gathering efforts. Due to the tight time frame of the test, only minimal processing was possible prior to compiling the sets and putting them into use on the test systems, so the sets scanned by each product contained well over 100,000 samples. We expected a great deal of these to be ruled out of the final count – whether because they failed our validation process or because they didn't even get as far as the checking process – but the large raw sets promised a significant amount of scanning time and the likelihood of problems for the products. In the final reckoning, the weekly batches averaged just over 12,000 samples per week.

The speed sets, used for our various performance measures, were tidied a little but remained much the same as usual. Some minor adjustments were made to the CPU and RAM usage measurement tools introduced recently (for a full explanation of these see *VB*, April 2010, p.23). With everything in place, testing proceeded without delay.

Agnitum Outpost Security Suite Pro 2009 6.7.3

ItW 100.00%

Polymorphic 89.10%

ItW (o/a) 100.00%

Trojans 90.35%

Worms & bots 95.88%

False positives 0

Agnitum's Outpost has put in a string of solid performances of late; it has a straightforward and unflinching approach providing several protective layers in a well-ordered, solid-feeling interface. Set-up and configuration is clear and problem free, with a reboot required to complete installation. Chugging through the test sets proved equally smooth and reliable. Scanning speeds were not lightning fast, but some good optimization improved the speed of scanning of previously checked items considerably. This made for a good profile on our speed graphs, while RAM consumption was a little above the average for this month's field, but CPU cycle drain was fairly low, even under heavy pressure. Detection scores in the main sets were very solid, and RAP scores fairly decent. With no problems handling the WildList and no false alarms in the clean sets.

AhnLab V3Net for Windows Server 7.7.6.4 build 1152

ItW 100.00%

Polymorphic 99.58%

ItW (o/a) 100.00%

Trojans 67.43%

Worms & bots 69.43%

False positives 0

The set-up process for the server version of *AhnLab's* product is fast and simple, with few decisions to make and no need for a reboot to complete. The product interface closely resembles the desktop edition, with a fairly minimal set of configuration options which might be a little short on flexibility for more demanding administrators. However, navigation is clear and tidy and carrying out simple tasks is easy, with the available options well laid out. The separation of scans into virus and spyware checks was a little confusing however – most products offer a separate spyware system which looks at registry entries and other configuration issues rather than scanning files; it seems more rational to keep it simple and check for any bad stuff with a single scan, rather than requiring multiple checks.

Running through the tests, the on-access scan of the main set brought up our first blue screen on the new platform – this came after a rather longer period of stability than on our first visit to *Windows 7*, but was still rather disappointing. The machine rebooted happily though, with nothing vital lost by way of logging etc., and retries proved more successful with no repeat of the glitch. Scanning speeds were mid-range on demand, with a small amount of optimization evident in the 'warm' scans, and pretty impressive on access. RAM usage was fairly low and CPU consumption around the middle of the field. Detection rates in the main test sets were unspectacular, and the RAP sets were not handled especially impressively either. It has been suggested that our sample-gathering techniques may put vendors from certain geographic regions at a disadvantage, but we have been making every effort to ensure global coverage and some of our largest and most regular sample sources are based in the Far East – we will continue to work on this issue to improve the representativeness of our test sets.

The WildList and clean sets proved no problem for *AhnLab*, however. There were a large number of alerts stating that *Office* documents containing macros contained, well, macros, but the warnings were couched in language that was close enough to a detection alert to merit recording them in the 'suspicious' column on our tables. Nevertheless, *AhnLab* comfortably earns a VB100 award.

avast! Server 4.8.1113

ItW 100.00%

Polymorphic 99.33%

ItW (o/a) 100.00%

Trojans 93.56%

Worms & bots 96.93%

False positives 0

avast!(formerly *Alwil*) announced the change of its company name as testing got under way – this seemed like a sensible move given the product’s brand recognition value. Disappointingly, the company name was the only new thing here – the developers informed us that the new version 5 server edition of the product was not quite ready for release, and we had to make do with version 4. This was no great problem, however, as the older edition has been around long enough to acquire a rugged stability which shrugs off the need for flashy good looks. The installation process is lucid and logical, and after a reboot the slightly unusual control system provides an admirable level of configuration – enough to satisfy the most demanding of administrators.

Running through the tests was a smooth process, with excellent scores in the main sets and RAP scores perhaps a fraction below what we have seen in recent months – clearly version 5 includes some significant improvements in more than just the GUI design. Scanning speeds were pretty zippy though, and both file access lag times and RAM consumption very light indeed.

AVG Internet Security Network Edition 9.0.814

ItW 100.00%

Polymorphic 97.57%

ItW (o/a) 100.00%

Trojans 96.74%

Worms & bots 98.01%

False positives 0

AVG’s developers chose to submit a standard Desktop product for this test, rather than the specialist server versions many of their fellow vendors provided. The flagship product installs quickly and easily, with no need for a reboot despite the multiple layers of protection included (many of which are not covered by our testing but should provide additional defence against attacks). As we have noted previously, the presentation of the many modules has some redundancy and makes the GUI a little cluttered and on occasion confusing to navigate, but there is a solid and respectable look and feel to it, and a good level of fine-tuning is provided for most purposes. Scanning speeds were fairly average, on-access lags low in some areas but heavier in others. RAM usage was low, but CPU consumption fairly high, making for a mixed set of performance results overall. Detection rates in the main test sets were exemplary and RAP scores were pretty impressive.

Avira AntiVir Windows Server 8.02.01.211

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 96.96%

Worms & bots 98.11%

False positives 0

Avira's AntiVir provided the first of what we expected to see many of this month: fully fledged server protection systems based on the MMC system. Installation was delayed a little thanks to the requirement for C++ libraries to be put in place, but no reboot was needed to finalize the install. The interface is, of course, considerably more demanding than the average cartoony home-user GUI, but provides a complete range of controls and fine-tuning options. These are fairly easy to locate and configure once the layout and operation technique have been divined.

Scanning speeds were consistently fast, with some good, light on-access times, low CPU drain but surprisingly high RAM usage. Once again some excellent scores were recorded across the standard sets and also in the RAP sets. Full coverage extended to the WildList set, and with no false alarms.

BitDefender Security for Windows Servers 3.4.11.141

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 93.17%

Worms & bots 92.87%

False positives 0

Another full-blown server solution, and again using the MMC for its main control interface, *BitDefender's* product installed simply and proved equally straightforward to operate – with rather more colour and panache to the GUI than expected from this kind of approach. Navigation was logical and the scheduling system in particular drew approving nods from the lab team, with a quick and simple set-up process for jobs using a proper calendar for improved efficiency. A few oddities were noted in some jobs, with a number of subfolders of the selected areas apparently skipped over in some scans, but after careful checking and a few re-runs, a complete set of results were safely in the bag.

Scanning speeds were pretty good on demand and not bad on access once the product had familiarized itself with the files; the resource usage graph also shows a pretty light memory and processor footprint. Some highly respectable detection figures were obtained in the main sets, with decent coverage across the RAP sets too. The WildList was handled effortlessly, and with no false alarms

Bkis BKAV Gateway Scan 2829

ItW 100.00%

Polymorphic 63.21%

ItW (o/a) 100.00%

Trojans 50.00%

Worms & bots 69.09%

False positives 4

Bkis BKAV Gateway Scan Plus 2829

ItW 100.00%

Polymorphic 63.21%

ItW (o/a) 100.00%

Trojans 50.00%

Worms & bots 69.09%

False positives 4

Bkis BKAV Home Edition 2829

ItW 100.00%

Polymorphic 54.25%

ItW (o/a) 100.00%

Trojans 50.00%

Worms & bots 69.09%

False positives 4

Bkis BKAV Home Edition Plus 2829

ItW 100.00%

Polymorphic 58.17%

ItW (o/a) 100.00%

Trojans 50.00%

Worms & bots 69.09%

False positives 4

Bkis made its VB100 debut in the last comparative and put in a good showing but didn't quite make the grade for certification. Clearly encouraged by the experience, the company has returned in force this month with no fewer than four products submitted. Despite our warnings that it might not be possible to include so many in what looked likely to be a well-subscribed test, as well as the recent imposition of entry fees for three or more submissions from a single vendor, the Vietnamese firm insisted they all be included, and in the end – thanks to generally good behaviour – we managed to squeeze them all in. As all are fairly similar both in design and in performance, it seems sensible to cover them all with a single write-up, pointing out any differences as necessary.

The installation process is remarkably simple, with only a couple of clicks and a few moments' wait before everything is done – a reboot is needed at the end. The interface is clear and well laid out, providing a basic level of configuration. This is unlikely to satisfy the demands of a corporate server administrator, but ample for the average inexpert home user. The only evident difference between the home and gateway versions – on the surface at least – is the colour of the interface, which is a slightly pastel orange for the home products and a rather sickly green for the gateway ones.

Running through the tests proved fairly straightforward thanks to the simple and responsive design, and the absence of any serious problems. Detection rates for all products were fairly similar, with some evidence of improved coverage of polymorphic viruses in the gateway solutions.

Scores in the main sets were somewhat below par, and in the RAP sets showed a severe dip in the week -2 set, recovering slowly to show a surprising jump in the proactive week – we can only assume that some oddity in the sources of our sets caused the latter two weeks of the reactive portion to contain a large number of items not accessible to *Bkis*.

In the performance tests, all four products were closely matched in terms of scanning speed (somewhat mediocre) and lag times (rather hefty). In the resource consumption measures, the *Gateway Scan* product showed some pretty high use of RAM throughout, while all the others were much lower on the same measure, performing quite favourably compared to the field. However, all were fairly high on CPU cycle consumption.

After a handful of misses in the WildList last time around, things were looking good when all four product versions managed a clean sweep of the latest list in both modes. An unlucky snag arrived in the clean sets however, when all four identified a tool provided by *Microsoft* as a Trojan (several versions for different platforms were included in the clean set), and also misidentified another item from a prominent developer, thus denying *Bkis* its first VB100 award for a second month running.

In a final unexpected difference between the four products, one of them labelled a large swathe of samples included with the core operating system as suspicious adware. Despite these glitches *Bkis*'s product range impressed with its stability and good behaviour, and the company remains a strong contender to join the ranks of VB100 certified vendors soon.

Central Command Vexira Anti-Virus for Windows Servers 6.2.53

ItW 100.00%

Polymorphic 89.10%

ItW (o/a) 100.00%

Trojans 90.24%

Worms & bots 95.95%

False positives 0

Vexira entered our mammoth *XP* test after a lengthy absence from the comparative reviews, and returns this month for more of the same. The product set-up is reasonably undemanding, and on completion we were not surprised to see the familiar interface of *VirusBuster*'s server solution, veteran of many server-level comparatives, with a change in colour scheme apparently the main difference.

The GUI itself – once again using the MMC system – is a little clunky and awkward in places, lacking a little in completeness of vision with some options looking the same, but operated in different ways. In general, a good level of control is provided once the control system has been wrestled into submission, but in some places it is less than fully effective – notably, the options to enable on-access checking of archives appeared to have no effect at all.

Scanning speeds were fairly middling, with no sign of any optimization on repeat scanning and a fairly low resource footprint, but detection rates were respectable in the main test sets and pretty decent in the RAP sets too.

Coranti Multicore 2010 1.000.00022

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 96.48%

Worms & bots 98.72%

False positives 0

A newcomer to the VB100 test bench, *Coranti* is the new face of a project which, under a different name, has been on the verge of joining the tests for some time. Still in beta, the product uses a multiengine approach combining the detection capabilities of four separate solutions. First impressions were good, with a clean and smooth installation process which zipped through, although the initial update of all four engines did take quite some time, with something close to 250MB of data to download. This could present difficulties in some situations, and it might be preferable for the developers to provide their installer to customers with more recent detection data included, rather than making them install the product and then leave their machine less than fully protected for such a long time. Perhaps this will be implemented as the development process draws to completion.

The product interface is attractive and nicely laid out, with a decent level of configuration easily accessible. While running a scan, an animation shows a magnifying glass moving over an orange symbol – although at first glance this looked like someone polishing a gold fish. A few quirks were noted, most frustratingly the apparent inability to return to the scan progress screen if navigated away from mid-scan. These were minor issues though; scanning speeds were rather more of an issue, with the multi-engine approach apparently running each engine in turn over the selected area, making for multiple progress bars and some rather lengthy scanning times. File access lags were rather hefty too, and as might be expected, use of CPU and RAM was among the highest in this month's field.

The flip side of this, of course, is the power of multiple engines, and unsurprisingly some splendid scores were achieved across the test sets, with very solid numbers in all the RAP batches. This information was a little hard to come by, with logs having to be stripped from a rather gnarly database format, and hopefully future builds will include the option to keep all detection data and export to file – an especially important option for anyone using the product in a proper server environment.

The WildList set was handled without problems, and in the clean sets, where there was some danger of the multi-engine approach causing further problems, only a handful of suspicious warnings were raised, meaning *Coranti* can proudly join the ranks of VB100-certified products.

Defenx Security Suite 2010 3063.452.0728**ItW** 100.00%**Polymorphic** 88.85%**ItW (o/a)** 100.00%**Trojans** 89.83%**Worms & bots** 95.75%**False positives** 0

Another relative newcomer returning after a successful debut last time around, *Defenx* is closely modelled on *Agnitum's Outpost* product, with a change of colour scheme the main adjustment made for the company's regional users.

The set-up and usage experience are thus identical to that of *Outpost*, and speeds, performance ratings and detection scores also show little difference.

Good detection levels in the main sets and decent RAP scores combine with an absence of false alarms in the clean sets and fine coverage of the WildList to earn *Defenx* its second VB100 award.

Digital Defender 2.0.27**ItW** 100.00%**Polymorphic** 89.10%**ItW (o/a)** 100.00%**Trojans** 87.15%**Worms & bots** 94.50%**False positives** 1

Digital Defender is another of the newbies from the last test, returning after a glorious debut. Its solution is an implementation of the *VirusBuster* detection engine in a pleasantly simplified GUI – unlikely to appeal to most server admins but more than ample for the home market (which seems to be the company's main target). Installation and set-up is fairly straightforward, but testing was impeded initially by the requirement for an activation key to access some of the configuration. With this in place, things moved on reasonably well – hampered for a time by the overwriting of logs after a fixed level of entries, but this issue was circumvented and results eventually obtained. Scanning speeds and overheads were fairly good and performance drains pretty light, with some decent scores in the main sets. A solid start in the RAP sets was followed by a fairly sharp drop in the proactive week – notably more so than others based on similar technology, hinting at an entry made somewhat earlier than others and missing some last-minute updates. Also differing from others based on the same technology, a single false alarm in the clean sets – a guide to *Windows 7* produced by *Microsoft* flagged as an exploited document – meant that, despite a clean run through the WildList set, *Digital Defender* narrowly misses out on a VB100 award this month.

eEye Blink Server 4.6.2**ItW** 99.99%**Polymorphic** 82.01%

ItW (o/a) 99.99%

Trojans 75.10%

Worms & bots 72.76%

False positives 0

Blink has become a regular entrant in our tests lately, but this is the first appearance of the server edition. In terms of user experience there is not a great deal of difference however; the install process is fairly simple and speedy, and the interface looks much the same – fairly serious and unflashy with an air of solid efficiency. A decent level of configuration is provided, and the product seems to run smoothly and respond to adjustment rapidly. There are a number of additional protective layers, including the vulnerability management which is the firm's forte.

One oddity was noted when a large scan job, which ran for over 36 hours, came to an end without quite covering the full area requested, skipping over the last few folders. There was not enough time to retry the whole job, so just those sections of the test set that had clearly been missed out were re-scanned separately.

On-demand scanning speeds were rather languorous, thanks to the implementation of *Norman's Sandbox* to thoroughly investigate unknown items, and lag times and RAM usage were also fairly high, with CPU cycle usage in high activity periods considerably higher than most products. Detection rates were reasonable in most sets, with the clean set handled without problems, but in the WildList set a tiny number of examples of the W32/Virut strain which also caused the product problems last time went undetected. Although only falling short of the required 100% by a whisker, *Blink* misses out on a VB100 award once again.

eScan Internet Security Suite for Windows

10.0.1058.690

ItW 100.00%

Polymorphic 99.99%

ItW (o/a) 100.00%

Trojans 93.06%

Worms & bots 96.50%

False positives 0

The latest version of *eScan's* suite provides a number of additional protective layers not covered by our testing, but installs easily and is fairly simple to operate.

The logically designed interface provides a decent range of fine-tuning options in an easily accessible way. Scanning speeds were sluggish in the extreme on demand, with some optimization apparent on rescans in some areas but not in others.

On-access overheads were fairly low however, and resource consumption not too intrusive.

Detection rates were pretty solid, with high scores in the main sets and a decent showing in the RAP sets. The WildList caused no problems, and with no nasty surprises in the clean sets, *eScan* earns a VB100 award.

ESET NOD32 Antivirus 4.2.40.0

ItW 100.00%

Polymorphic 99.99%

ItW (o/a) 100.00%

Trojans 96.73%

Worms & bots 99.15%

False positives 0

Little has changed about *ESET's NOD32* for some time, only a few adjustments having been made since a major redesign a few years ago. It remains attractive to look at as well as easy to use. The installation process is fairly standard – enlivened only by the unusual feature of requiring the user to make a choice as to whether or not to detect greyware items – and does not require a reboot to complete.

The interface is clear and detailed, with an excellent selection of configuration options, some of which are a little repetitive in places but generally logically and clearly laid out. During testing the interface appeared to freeze up a few times when asked to do more work while under heavy stress, but it soon recovered its composure and continued to get on with the job under the hood.

Scanning speeds were medium, with on-access lags and CPU usage also in the middle of the field; memory usage was fairly low, however. Detection rates were excellent, showing a continuation of the upward trend seen in the last few tests. A couple of items in the clean set were alerted on as potentially unwanted – a fairly accurate description of toolbars and other functions bundled with popular freeware packages – but no false alarms were noted and the WildList was handled flawlessly, earning *ESET* yet another VB100 award.

Fortinet FortiClient 4.1.3.143

ItW 100.00%

Polymorphic 99.08%

ItW (o/a) 100.00%

Trojans 70.61%

Worms & bots 89.64%

False positives 0

Fortinet's endpoint client seems fairly unchanged from several recent tests, although during the simple and speedy install an option to select a free or premium version of the product was something of a surprise. The interface is nice and clear and provides a fair degree of configuration, but a few problems were noted during testing; on-access scanning appeared initially to be inactive, but after a reboot (not demanded by the installer) this was rectified. Also, an attempt to run some jobs on the scheduler failed to produce any scanning.

Further upsets were to follow, with both on-demand and on-access tests freezing and hanging frequently throughout scanning of the trojans and RAP sets. Some samples in the test sets appeared to trip up the engine, meaning that during the on-access tests the machine would occasionally start moving extremely slowly, while it was clear that all on-access detection had ceased. Oddly, after several forced reboots and continuations with the offending portions of the sets removed, we eventually found that

protection could be restored simply by switching the on-access protection off and back on again (no easy task given the state of the machine, with every click taking an age to have any effect and the whole experience feeling like pushing a bus with no wheels up a steep slope). As the on-access tests would continue while this process was performed, it may have caused some samples to go undetected which would have been spotted had the product been fully functional, but given the time already taken up there seemed to be no other option.

The RAP tests were even more problematic, with numerous attempts to get through the sets failing, including one overnight attempt which stuck after about 500 samples and sat there all night insisting it was still scanning but making no further progress – the task had to be forcibly killed to allow further interaction with the product. Blocks of samples had to be removed to obtain complete results.

Scanning speeds were obtained, which were fairly decent, with mid-range overheads and resource consumption. Detection results for the main sets also proved reasonable, given the somewhat anomalous figures for the trojans set; the low RAP scores may suffer from the same effect. With the WildList and clean sets handled without problems, the product just about scrapes through to earn a VB100 award, but admins will be well advised to keep a close eye on the product to ensure it doesn't get itself snarled up.

Frisk F-PROT 6.0.9.3

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 98.26%

Trojans 79.41%

Worms & bots 92.41%

False positives 0

Frisk's product remains simple in the extreme, with an installation process which completes quickly in only a handful of stages; a reboot is required to complete.

The pared-down interface provides a basic set of controls, and its simplicity makes it hard to get lost in, but does have a few odd little quirks which may confuse users who are not used to the design.

Testing proceeded smoothly, with some good scanning speeds recorded and no complaints about the on-access overheads either; memory use was fairly low while quite heavy use was made of CPU cycles. Scanning the main sets produced some decent scores, but in the RAP sets the product reported errors several times, on occasion requiring a reboot to return the scanner to a usable state. On-access protection remained stable throughout despite these problems. RAP scores, once fully obtained, proved pretty decent, and all was well in the clean sets. The WildList was handled well on demand, but despite all looking good, one more fly appeared in the ointment on checking the on-access results – a handful of samples, detected without problems on demand, were ignored by the on-access scanner. The fact that these samples were all detected on demand with the same detection ID hints at some error in the set-up of the on-access component. A VB100 award remains just out of *Frisk's* grasp this month.

F-Secure AntiVirus for Windows Servers 9.00 build 333

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 93.03%

Worms & bots 93.43%

False positives 0

F-Secure's server-level product installs fairly simply, with no reboot requested,

Although we chose to restart the machine as a precaution after manually applying updates. The interface is web-based, which caused some rather disconcerting alerts from the locked-down browser warning of untrusted sites and defunct certificates; doubtless these problems would be mitigated on a system with a web connection (which not all servers will necessarily have).

The design of the interface is clear and it looks attractive, but the scan design is somewhat clunky and the scheduler system is fairly basic. Only a single job can be set up with the standard settings of the manual scanner – more demanding admins may want considerably more flexibility to run various scheduled jobs – and even selecting more than a single folder is not at all simple.

We also noticed on a few occasions the manual scanner settings reverting to previous options despite changes having apparently been applied successfully.

With these quirks observed and noted, scanning proceeded fairly well, with some excellent speed measures, fairly light resource usage and decent scores in the main sets on access. On demand, however, we found logging something of a problem – an issue we have noted before with *F-Secure* products. Twice we ran the standard large job scanning the usual selection of test sets, but on both occasions although the results screen showed large numbers of detections, clicking the 'show log' button brought up details of the previous scan – a clean job with nothing to report. In the end, a command-line version of the scanner bundled with the product was used to get results, and the issue seemed only to affect scans with large numbers of detections. This may be an unlikely scenario in the real world, but is not inconceivable in a large file server environment – most server administrators will want considerably more detailed, trackable, and most of all reliable logging from a serious server-grade product.

The developers have made some urgent investigations into the problems we encountered and have promised a rapid fix.

Despite our logging issues, detection rates across the sets proved very solid, and with no problems in the WildList or clean sets *F-Secure* earns a VB100 award.

G DATA AntiVirus 10.5.132.28

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 99.33%

Worms & bots 93.82%

False positives 0

G DATA's server product has appeared in a previous comparative with only German language interfaces, but this time a full translation was provided, allowing much more thorough investigation of its capabilities. The set-up process is slightly complex, with an administration element installed first and the client protection deployed from there. This seemed a very proper approach to corporate usage, and worked fairly well. Some error messages were shown during the installation of the management tool, related to the .NET and SQL Server components bundled with it, but these seemed to present no serious problem. Everything was soon up and running, and deployment of the client protection ran very smoothly and simply.

Running through scans was fairly easy too, with some excellent optimization of scanning of previously checked files and a surprisingly light imprint on memory and processor cycles. Occasionally the connection to the admin tool was lost and had to be re-initialized, and on completion of large scan jobs we had some problems exporting logs to file, with the export function failing silently on several occasions. Eventually we gave up on it and resorted to ripping the data from some temporary cache files uncovered by digging through the registry.

The data obtained showed the product's usual superb detection levels across all sets, with no issues in the clean or WildList sets, and *G DATA* earns a VB100 award despite a few frustrations in the product.

Kaspersky Anti-Virus 6 for Windows

Servers 6.0.4.1424

ItW 100.00%

Polymorphic 99.99%

ItW (o/a) 100.00%

Trojans 94.99%

Worms & bots 98.33%

False positives 0

Kaspersky Lab entered two products this month, the first apparently being the Current standard product.

The install and set-up is a fairly simple and painless process, and the interface is another based on the MMC, with some nice use of colour to give it a little clarity.

It proved fairly easy to use if somewhat complex, and provided an excellent level of configuration for the server administrator.

Scanning speeds were good, with previously scanned files effortlessly ignored, resource usage on the low side and detection rates excellent. The only oddity noted was an apparent rescan of infected sets after the job had completed together with a prompt which asked for an action, but this did not affect the gathering of results once the scan was aborted.

The WildList and clean sets were handled well, and a VB100 award is comfortably earned.

Kaspersky Anti-Virus 8 for Windows Servers Enterprise Edition 8.0.0.354

ItW 100.00%

Polymorphic 99.69%

ItW (o/a) 100.00%

Trojans 94.70%

Worms & bots 98.37%

False positives 0

The second offering from *Kaspersky* this month is a new version, which appears to be in a late stage of beta testing.

The install and set-up was a little more complex than the older version, with both a protection client and an administration tool required, but once up and running the MMC interface met with approval from the lab team, who considered its design one of the best approaches to the format seen this month.

The only slight annoyance was the fiddliness of setting scan options, with actions stored in a separate area from the main set-up component, but this was soon dealt with.

Scanning speeds were once again excellent and benefited hugely from smart optimization with both memory and CPU usage slightly higher than version 6, but barely noticeably.

Detection rates were also splendid, although RAP scores were a little down on the other product – presumably due to some heuristic approaches not being included with this version. The WildList set caused no problems though, and the few alerts in the clean set accurately labelled VNC clients as VNC clients – useful information for a corporate admin. *Kaspersky* earns a second VB100 award this month.

Kingsoft Internet Security 2011 Advanced Edition 2008.11.6.63

ItW 100.00%

Polymorphic 57.11%

ItW (o/a) 100.00%

Trojans 15.03%

Worms & bots 35.93%

False positives 0

Kingsoft's latest product installs very simply in just a few clicks, with no need for a reboot.

The design is glossy and attractive, but only provides basic configuration and is a little clunky in translation at some points.

Scanning speeds were reasonable, with a fairly light impact on system performance, but detection rates over recent items were fairly disappointing – although, bizarrely, the proactive week of the RAP sets was handled better than the older samples. No problems were spotted in the WildList or clean sets however, and a VB100 award is duly earned.

Kingsoft Internet Security 2011 Standard Edition 2008.11.6.63

ItW 100.00%

Polymorphic 57.11%

ItW (o/a) 100.00%

Trojans 10.46%

Worms & bots 31.63%

False positives 0

Once again *Kingsoft* provided two products that are almost indistinguishable on the surface, with nothing to indicate which is the standard and which the advanced, other than the name of the installer.

The installation and user experience were identical, with even more lamentable detection rates in many of the sets, but the certification requirements were met comfortably and *Kingsoft* earns a second VB100 award this month despite a rather poor RAP showing.

McAfee VirusScan Enterprise 8.7.0i

ItW 100.00%

Polymorphic 99.99%

ItW (o/a) 100.00%

Trojans 85.84%

Worms & bots 93.69%

False positives 0

McAfee's corporate product is an old faithful, remaining pretty unchanged for many years now, but there seems no need to mess with such a solid and business-like tool.

Installation is fast and simple, requesting a reboot to engage some of the network protection but not requiring it to get the core malware protection enabled.

Running through the tests was as smooth and efficient a process as ever, with decent scanning speeds, on-access overheads and CPU use somewhat above average, but memory consumption the lowest of all products tested this month.

Detection rates were similarly reliable across all sets, with no problems in the WildList or clean sets, thus *McAfee* earns a VB100 award and extra commendation for solidity and problem-free testing.

Norman Endpoint Protection 7.20

ItW 99.99%

Polymorphic 83.09%

ItW (o/a) 99.99%

Trojans 74.87%

Worms & bots 72.57%

False positives 3

Norman's server product installs in a few standard steps and needs no reboot to get down to business.

The interface is closely modelled on the desktop versions seen in previous comparatives, with a fairly simple design and a fair level of options for the server admin, laid out in a rational and intuitive manner.

With the heavy use of the firm's renowned sandbox for additional protection against new threats, scanning speeds were fairly sluggish, particularly over executables, and on-access overheads and resource usage similarly high.

Detection rates were reasonable in the main sets and the RAP batches, but in the WildList set – as feared having already seen the results of other products using the *Norman* engine – a tiny number of W32/Virut samples went undetected.

In the clean set, a batch of files included in the *Sun Java* SDK were detected as, of all things, JAVA/SMSsend.B trojans, making doubly sure that no VB100 award can be earned by *Norman* this month.

Quick Heal AntiVirus 2010 Server Edition 11.00/4.0.0.3

ItW 100.00%

Polymorphic 99.50%

ItW (o/a) 100.00%

Trojans 76.95%

Worms & bots 89.49%

False positives 0

Quick Heal's server edition seems little different from its desktop versions, with the usual fast and simple install process with no reboot needed. The interface is similarly simple to use, and ran stably throughout the test. Scanning speeds were pretty good, and on-access overheads fairly decent too, with a surprisingly high amount of RAM used but CPU use lower than many in this month's field.

Detection rates were reasonable in the main sets, a little below par in the RAP sets, but the core requirements of the clean sets and WildList samples were handled flawlessly, and a well-behaved product earns *Quick Heal* another VB100 award.

Rising Internet Security 2010 22.00.02.96

ItW 100.00%

Polymorphic 70.27%

ItW (o/a) 100.00%

Trojans 48.78%

Worms & bots 58.41%

False positives 0

Rising's 2010 edition is colourful and cartoony, with an installation process of average length and complexity.

The GUI provides a decent level of configuration, which is mostly fairly accessible but in places it can be a little laborious to implement certain changes. Some nice graphs and other statistical data are provided alongside the standard logging subsection.

On-demand scanning speeds were unspectacular, and on-access overheads fairly high, with impressively low memory consumption and CPU usage remarkably high.

Detection rates across the sets were fairly mediocre, with RAP scores tumbling as the samples grew more recent, but the WildList was handled without difficulty and no problems emerged in the clean sets either, thus earning *Rising* another VB100 award.

Sophos Endpoint Security and Control 9.0.5/4.52G

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 91.22%

Worms & bots 98.25%

False positives 0

Sophos's latest offering remains little changed from previous versions, with numerous new features stealthily merged in without any major redesign of the interface. The interface itself is fairly simple to navigate and provides a truly remarkable degree of fine-tuning, much of it located in a super-advanced area which we refrained from meddling with. Installation is simple and clear, and completed rapidly with no requirement for a reboot.

Performance tests showed some fairly average scanning speeds and on-access overheads, and pretty low resource consumption. Running the main detection tests was a little more problematic however, after an initial attempt to run a scheduled scan overnight failed with cryptic error messages hinting at a lack of space. Attempting to open the product's log file drew the same error, although the system partition had at least 20GB free – surely plenty to allow a log to be loaded.

A reboot quickly put a stop to this silliness and tests proceeded without further interruption, although not as quickly as the progress bar would have us believe (as in many previous tests, it quickly leapt to 99% and remained there for well over 99% of the scanning time).

In the main sets detection rates were excellent, but a first stab at the RAP sets showed some bizarrely low and irregular figures. A retry showed the scanner getting stuck on a file on at least a couple of attempts, and in the end results were obtained with the offending item removed from the set, and using the command line scanner provided with the product for speed (considerably more than the allotted time having already been taken up). Results proved well worth the wait however, with excellent scores across all four weeks, the proactive week particularly impressive.

The WildList and clean sets caused no difficulties though, and *Sophos* also earns another VB100 award.

SPAMfighter VIRUSfighter 6.101.6

ItW 100.00%

Polymorphic 71.61%

ItW (o/a) 100.00%

Trojans 87.09%

Worms & bots 88.82%

False positives 1

Yet another repeat appearance from one of last month's newcomers, *VIRUSfighter* is one of many implementations of the popular *VirusBuster* engine. A simple and rapid installation process requires no reboot and results in a fairly attractive interface which is reasonably simple to operate. A pretty limited set of controls is provided – suitable for the home user but unlikely to appeal to the server administrator. On-demand scans from the GUI can only target whole disk partitions, so most tests were run using the context-menu option.

Running some of the larger detection tests proved a little problematic, with scans failing, hanging or crashing a number of times. On some occasions the product reported that scanning was still ongoing long after the logs showed having reached the end of the sets – which made it a little tricky to guess when something was, in fact, finished. Detection results in the main sets and RAP batches were reasonable, more closely mirroring *Digital Defender* (with which the product shares some ancestry) than the core *VirusBuster* product on which it is ultimately based.

While the WildList was handled adequately, as expected, a single item in the clean sets – that pesky *Microsoft* howto document – was labelled as exploited, and as a result *SPAMfighter* narrowly misses out on a VB100 award this month.

Trustport AntiVirus 2010 5.0.0.4118

ItW 100.00%

Polymorphic 100.00%

ItW (o/a) 100.00%

Trojans 97.55%

Worms & bots 98.95%

False positives 0

Trusty *Trustport* is put in place with a fairly fast set-up process, and provides a sturdy, business-like interface.

A very good amount of configuration and fine-tuning is offered, which is arrayed sensibly to allow easy access to all the required options. Running through the tests was smooth and simple, although the product's dual-engine approach caused the scans to be somewhat slower than most, with on-access overheads and resource consumption somewhat higher.

However, detection rates were pretty stratospheric, with an awesome display in the RAP sets which could well be our highest ever score. The WildList presented no difficulties, and with no false alarms either *Trustport* romps home to another easy VB100 award.

VirusBuster for Windows Servers 6.2.51

ItW 100.00%

Polymorphic 89.10%

ItW (o/a) 100.00%

Trojans 90.24%

Worms & bots 95.95%

False positives 0

We have already seen the *VirusBuster* engine in use several times this month, and even the interface for this server edition made an appearance earlier in the *Vexira* product. The MMC-based system provides a reasonable degree of control, although many of the controls are somewhat fiddly to operate and there is a lack of consistency in the implementation. Monitoring the progress of jobs is also somewhat problematic.

Nevertheless, testing progressed without any major obstacles, and results were much as expected, with a decent showing in the main sets, reasonable scores in the RAP sets and mid-range performance figures. No problems were encountered in the WildList or clean sets, and *VirusBuster* proves worthy of a VB100 award this month.

CONCLUSIONS

It proved to be another somewhat exhausting test this month, with pressure on the lab team not helped by some illness during the course of the month, and the attendance of technical meetings and conferences abroad. This would have been less of a problem had the products played nicely and behaved as well as we had hoped. With a tight schedule and limited testing resources, we allocated an ideal 24 machine/hours per product – we felt that this was not an unreasonable estimate of the time it should take to complete all the required tests, and many products easily got through all the sets and the various iterations of the performance measures within this time period.

However, several other products were less than cooperative. Many an evening we left the lab fully expecting to find several sets of completed results by morning, only to be disappointed on our return with products stuck on odd files, claiming completion but actually having skipped chunks of the sets, or completed but having failed to record accurate results of what they had been up to. A further handful of products submitted to the test took up their share of testing time – and in some cases more than their fair share – but in the end were excluded from the test due to various problems: incompatibility with the test platform, problems applying updates, or difficulties obtaining enough usable results for it to be worthwhile including them.

These inconsistencies and unreliable behaviours are particularly significant on a server platform, where administrators require absolute trustworthiness and total trackability of all activities, especially regarding detections and attempts at disinfection. In many products this month – even those claiming to be aimed at the server sphere – we noted shortcomings in configuration as well, with some vital tools and options required by many admins either missing or not fully functioning.

Of course, a number of the products included in this test provide a range of additional capabilities not covered by our tests, but in the server environment much of the purpose of implementing a security solution is to protect things other than the server operating system itself – scanning and monitoring file shares and other inter-node

connections is vital to prevent cross-contamination, the passing of malicious code from one zone to another – and for such purposes the behavioural layers added to many of the products will be unsuitable. Even some of the cloud-based data provided by some solutions may be inaccessible on a server, depending on the strictness of corporate network set-up. This, then, is one area where ‘traditional’ detection technology remains at the forefront of the protective arsenal. We hope the data provided this month will be a useful resource to assist admins in selecting a suitable product for their purposes.

Among those products which did perform adequately in this test, we saw a fairly wide spread of results. Our performance measures highlighted a range of different approaches, with some using more or less memory than others, some more or less processor cycles; some used more of one than the other, while some were notably high or low on both counts. These performance figures should not, of course, be extrapolated to guess at the exact resource footprint in other circumstances or on other systems (where results could vary considerably), but they should provide a reasonable comparison between the products included in the test.

As far as detection rates are concerned, we have seen some really excellent figures in this test, with several products surpassing expectations while a few have done somewhat less well than expected. Our RAP data and charts also continue to provide plenty of interest.

We will continue to monitor the ever-changing abilities of labs to keep up with the growing glut of malicious code, returning to a desktop platform next time around and doubtless seeing another large haul of competitors on the test bench. We can only hope, for our sanity’s sake, to see some rather better behaviour than that encountered in many solutions this month.

Technical details

All tests were performed on identical systems with *AMD Phenom II x2 550* processors at 3.11 GHz, 4 GB RAM, and dual 80 and 500 GB SATA hard drives, running *Microsoft Windows 2008 Server R2 Standard Edition*.