COMPARATIVE REVIEW

WINDOWS SERVER 2008

John Hawes

The comparative review moves to an entirely new platform this month: the server version of *Microsoft*'s latest iteration of *Windows*. With the official release of the platform having been in February, there should have been plenty of time for developers and QA teams to ensure their products were fully integrated with the new environment.

This month's testing schedule saw a number of new challenges in addition to the usual time pressures and resource limitations. The breaking in of a new member of the testing team coincided happily with a series of significant adjustments to the standard line-up of testing tasks, more on which shortly. The range of products taking part continued to reflect the steady increase in diversity in the market. As always, the team entered the test lab hoping for smooth and speedy testing, but anticipating the gamut of problems including bizarre design, bewilderingly absent functionality and disappointing instability.

PLATFORM AND TEST SETS

The *Server 2008* platform shares a code base with *Vista*, with many tweaks and improvements in a variety of areas, but sensibly avoiding the rather showy and resource-hungry cosmetic adjustments which most users will identify with the new breed of *Windows* systems. The installation process follows the usual series of steps. Following the standard *VB* methodology, things were kept as simple as possible, with simple fileserver functionality added from the list of models available. Some driver software was required to activate networking and to get the most out of the graphical capabilities of the hardware in use, and some archiving tools were also installed to simplify the unpacking of the submissions, which as ever took on a wide range of formats. Unlike in the *Vista* desktop tests, no adjustments were made to the user set-up, and a user with administrative rights was logged in for all testing purposes, assuming that server administrators would need such rights to install core software to a system. With these tasks carried out, and a few tweaks to the display and desktop made for comfort and efficiency, images were taken of the identical systems and the test sample sets copied to the secondary hard drives ready for testing to begin.

As mentioned, the test sets saw some considerable evolution this month. Starting with the core of the VB100 sets, the WildList set was aligned with the July issue of the WildList, released about a week before the product submission deadline (2 September). The changes in the list from that used in the previous test included the disappearance of large numbers of older items, only to be replaced by an impressive swathe of new arrivals, the vast majority of which were trojans that target online gamers and most of these go by the fairly straightforward title of 'W32/OnlineGames'. A few of the more interesting items on the list were removed, including several of the W32/Virut variants, but enough of these highly polymorphic viruses remained to provide a frisson of danger for those products which had previously had difficulties providing full coverage of these items.

In the clean test set, a fairly large update was made with a swathe of software added. This included a selection of drivers and system tools acquired as part of the process of enabling the test systems and the new platform to interact, as well as a collection of packages downloaded as freeware or trial installations, this month focusing on web development tools. These enlargements of the test set were designed in part to expand the speed test collections, which are now approaching an acceptable size. The additions to the set were selected from software with reasonably significant manufacturers with reliable reputations, so were not expected to bring up a large number of false positives, but as ever with the growth of the set the chances of a mislabelling grew, and the older part of the set still seems to throw up occasional incidents.

The combination of these changes to the test sets with the new platform seemed to provide a pretty tough challenge for those vendors striving for the glory of a VB100 award, but we also paid attention to the additional information provided for our readers. The zoo collections saw another round of development towards a more flexible and relevant set of challenges, with the dwindling and less difficult test set of simple file-infecting viruses being retired to the legacy set for the time being. Replacing these was a substantial new selection of trojans, replacing entirely the set used in the last review with fresh samples gathered in the last two months. The set of worms and bots saw a small amount of updating, but we hope to implement a similar system of complete overhaul for each review in the near future.

Another upgrade was trialled this month, which is intended to add even fresher samples for each test, along with an element of retrospective testing to measure heuristic and generic detection capabilities. Preparations for this scheme – preliminary results of which we hope to present at the forthcoming *VB* conference in Ottawa – involved putting together a month's worth of new arrivals totalling well over 100,000 samples. The logistics of this looked set to be dwarfed by the difficulties involved in persuading a bevy of awkward and intractable products to produce usable results when scanning such a large set of samples in the very limited time available. Without further ado, we shut ourselves in the lab and got down to business.

Agnitum Outpost Security Suite Pro 6.5.2358.316.0607

ItW	100.00%	**Polymorphic**	75.64%
ItW (o/a)	100.00%	**Trojans**	75.67%
Worms & bots	99.93%	**False positives**	0

With this month's review running on a server platform, we expected most of the products to be dedicated to a server environment, but since many products designed for the desktop run quite happily in the same setting we accepted any such products which vendors saw fit to submit. First up on the roster alphabetically, *Agnitum* provided the same product as that entered successfully in several recent comparatives. Combining the company's own highly regarded firewall technology with a range of security extras including anti-malware detection provided by the *VirusBuster* engine, the product once again put in a solid performance, with a slick and well-designed interface and smooth, stable running.

Detection rates were reasonable, with somewhat below par coverage of the set of recent trojans but no problems in the WildList set. In the clean sets scanning times were fairly good, and an absence of false positives grants *Agnitum* its second VB100 in a row.

AhnLab V3Net 7.0.0.2

ItW	100.00%	**Polymorphic**	79.40%
ItW (o/a)	100.00%	**Trojans**	72.30%
Worms & bots	99.84%	**False positives**	0

AhnLab's *V3Net* product had some difficulties in the last comparative (see *VB*, August 2008, p.13), with the introduction of some engine upgrades causing some crashes during on-access scanning. The product provided for this test seemed pretty similar on the surface, with a simple and fairly attractive interface which kept some of its most useful controls hidden far away from where they might be expected to be found.

Some initial scanning results were safely obtained once the layout of the interface had been deciphered, but during on-access scanning of the trojan set blue screens were encountered, and repeated attempts to prevent this by the judicious removal of what were presumed to be offending samples proved fruitless. To get usable detection figures the set was eventually excluded from scanning entirely. By a chance mistake it was discovered that the list of executable file types did not include the .cmd extension used by some worms, which led to some worries until we found that the default setting was to scan all files regardless of type. The WildList was covered in full in both modes without further incident, and with speeds across the clean sets really quite good and false positives notably absent, *V3Net* makes the grade for a VB100 despite the wobbles.

Alwil avast! 4.8 Server Edition 4.8.985

ItW	100.00%	**Polymorphic**	92.25%
ItW (o/a)	100.00%	**Trojans**	94.20%
Worms & bots	99.78%	**False positives**	0

Bucking the trend seen so far, *Alwil* provided a server-specific product for this test. The interface showed little difference from that seen in recent desktop tests, other than by the fact that the rather funky pared-down interface provided by default in the desktop version was absent. However, this made little difference to testing, which generally requires the advanced options provided by the grown-up interface.

Detection rates across the sets were highly impressive as ever, and speeds were pretty good on demand, and reasonable on access. No problems were encountered covering the WildList, and without any false positives *Alwil* wins another VB100 award.

Arcabit ArcaVir 2008

ItW	90.58%	**Polymorphic**	86.54%
ItW (o/a)	90.58%	**Trojans**	66.48%
Worms & bots	99.44%	**False positives**	3

Arcabit returns once more to the VB100 test bench, having made its first appearance for several years in the last comparative review (*VB*, August 2008, p.13). The product was unchanged from last time, with the interface impressing with its simplicity and clarity of design. The developer's home market is hinted at by the fact that the option to switch into Polish is available from the system tray menu at all times.

Stability was similarly unimpeachable, even under the heavy strain of scanning large sets of new samples, and detection rates were fairly reasonable across the sets. However, a selection of samples recently added to the WildList were not detected, and in the clean set a small number of items were mislabelled as malware. Hence *Arcabit* does not qualify for a VB100 award this month, but continues to look likely to be a strong contender in the near future.

On-access detection rates	WildList viruses		Worms and bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Suspicious
Agnitum Outpost	0	100.00%	2	99.93%	393	75.64%	1242	75.67%		
AhnLab V3Net	0	100.00%	3	99.84%	703	79.40%	N/A	N/A		
Alwil avast!	0	100.00%	3	99.78%	290	92.25%	447	91.23%		
Arcabit ArcaVir	93	90.58%	8	99.44%	165	86.54%	1799	64.76%	3	
AVG	0	100.00%	1	99.95%	52	90.75%	478	90.63%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	52	98.98%	1	
CA eTrust	1	99.998%	0	100.00%	172	91.82%	3476	31.92%		
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	538	89.46%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	5000	2.06%		
Frisk F-PROT	0	100.00%	0	100.00%	125	95.66%	924	81.89%		
F-Secure	0	100.00%	0	100.00%	60	98.03%	466	90.87%	1	
Kaspersky	0	100.00%	0	100.00%	60	98.03%	287	94.38%	1	
Kingsoft	0	100.00%	16	99.10%	2119	41.19%	2605	48.97%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	216	95.77%		
Microsoft	0	100.00%	0	100.00%	141	95.02%	1054	79.35%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	122	96.00%	205	95.98%	1	
Norman Virus Control	0	100.00%	3	99.78%	1037	70.91%	788	84.56%		
Quick Heal AntiVirus	0	100.00%	45	95.16%	977	79.25%	3477	31.89%		
Redstone Redprotect	1	99.89%	0	100.00%	122	96.15%	481	90.58%	1	
Rising Antivirus	0	100.00%	4	99.64%	1333	60.04%	2260	55.73%		
Sophos Endpoint Security and Control	0	100.00%	0	100.00%	154	92.75%	625	87.76%		12
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	395	92.26%		
Trustport Antivirus	0	100.00%	0	100.00%	546	92.06%	155	96.96%		2
VirusBuster for Servers	0	100.00%	2	99.93%	392	75.77%	1281	74.91%		

AVG 8.0.169

ItW	100.00%	**Polymorphic**	90.75%
ItW (o/a)	100.00%	**Trojans**	94.96%
Worms & bots	99.95%	**False positives**	0

AVG also provided the same product for this test as for the recent *Windows XP* comparative: the most recent iteration of the company's suite as reviewed here a few months ago (see *VB*, March 2008, p.18). The new layout is something of an improvement on earlier versions, but remains a little awkward in parts, and getting everything running proved somewhat more fiddly than seemed strictly necessary.

Stability proved no problem throughout the main body of the tests, and although a few issues were observed when scanning the larger sets of infected items, it seems unlikely that such a situation would be very common in the real world. Detection rates were as splendid as ever, and speeds were on the good side of medium. With no false positives and no problems covering the latest WildList, *AVG* earns another VB100 award.

Avira AntiVir Server 8.1.0.1585

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.29%
Worms & bots	100.00%	**False positives**	1

Avira's server edition proved very different from the desktop version, with a console approach using the *Microsoft Management Console* as a base. This offered less straightforward access to such things as on-demand scans, as it is intended for sysadmins to set up regular scans of file shares to protect their networks rather than for the simpler

needs of the desktop user. However, configuration options were plentiful and reasonably accessible even for the demanding needs of a VB100 test run.

Detection rates were extremely high – approaching flawless, with the WildList detected effortlessly, and speeds likewise excellent across the board. Unfortunately, a single item in the clean set, which has gone many months without raising any suspicions, was labelled a trojan, and *Avira* thus does not qualify for a VB100 award this month.

CA eTrust ITM 8.1.637.0

ItW	99.998%	**Polymorphic**	91.82%
ItW (o/a)	99.998%	**Trojans**	26.35%
Worms & bots	100.00%	**False positives**	0

CA's *eTrust* product has barely changed in the last few years, with minor version changes little reflected in the product's layout or performance. Again intended more for sysadmins to set up and leave alone, the interface is not ideal for heavy interaction, but provides adequate tuning options for the VB100 test requirements. Implementation of archive scanning seemed not to function properly on access, despite an option to enable it, and logging as usual proved rather ungainly, with access to scan results from the interface itself all but impossible to use. The sluggishness of the interface was amplified by some difficulties scanning larger sets of infected items, which dragged to a halt on several occasions.

These things aside, scanning speeds were as remarkable as ever, and detection rates pretty decent in the more standard sets, if a little disappointing in the new trojans set. False positives were absent, but in the WildList a single sample of one of the W32/Virut variants was not detected, and thus *eTrust* does not make the required grade for a VB100 award this month.

ESET NOD32 Antivirus 3.0.672.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.00%
Worms & bots	100.00%	**False positives**	0

ESET's highly regarded flagship product was subjected to a major overhaul not long ago, and the stylish new look remains impressive both visually and in usability terms. Tweaking the controls to fit our needs was as usual a delight, and testing zoomed along at its usual rapid pace. Scanning of the extremely large new sets proved a little more sluggish, presumably as the product's strong heuristics kicked in, and on-access behaviour in the new trojan set was also a little odd, with many items not blocked on simple access but treated more severely when copying to the system or even browsing folders in *Explorer*.

Analysis of results showed the product's usual excellent detection rates and yet more splendid scanning speeds over the clean sets, and with nothing missed in the WildList set *ESET* adds yet another VB100 to its record tally.

Fortinet FortiClient 3.0.475

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	2.06%
Worms & bots	100.00%	**False positives**	0

Fortinet's product had a rather slow and lengthy installation process, and brought up one of the few query popups seen in this test, when *Windows* questioned the installation of a driver whose source it could not verify. Once up and running though, the interface presented few issues, being simple and straightforward and providing ample access to a wealth of configuration, as befits the more demanding requirements of a business environment.

Testing thus proceeded apace, with decent speeds and excellent stability even when scanning very large sets. Detection rates were as splendid as ever, but once again bizarrely let down by the trojan set, where detection was almost completely absent, leading to suspicions that some parts of the product were not fully functional. Nevertheless, with no false positives and full coverage of the WildList set, *Fortinet* gains another VB100 award.

Frisk F-PROT 6.0.9.1

ItW	100.00%	**Polymorphic**	95.66%
ItW (o/a)	100.00%	**Trojans**	85.39%
Worms & bots	100.00%	**False positives**	0

The *Frisk* product is simple in the extreme, with a very sparse and plain interface presented after the straightforward setup and obligatory reboot. Minimal configuration options kept work to a minimum, helped by zippy scanning speeds and low overheads, and detection was as usual excellent. A few crashes were observed while scanning large infected sets, including several during on-access scanning, but despite messages claiming the product had ceased to function it continued to block access to malware samples as if nothing had happened.

On-demand detection rates	WildList viruses		Worms and bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Suspicious
Agnitum Outpost	0	100.00%	2	99.93%	393	75.64%	1242	75.67%		
AhnLab V3Net	0	100.00%	3	99.84%	703	79.40%	1414	72.30%		
Alwil avast!	0	100.00%	3	99.78%	290	92.25%	296	94.20%		
Arcabit ArcaVir	93	90.58%	8	99.44%	165	86.54%	1711	66.48%	3	
AVG	0	100.00%	1	99.95%	52	90.75%	257	94.96%		
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	36	99.29%	1	
CA eTrust	1	99.998%	0	100.00%	172	91.82%	3760	26.35%		
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	561	89.00%		
Fortinet FortiClient	0	100.00%	0	100.00%	0	100.00%	5000	2.06%		
Frisk F-PROT	0	100.00%	0	100.00%	125	95.66%	746	85.39%		
F-Secure	0	100.00%	0	100.00%	60	98.03%	466	90.87%	1	
Kaspersky	0	100.00%	0	100.00%	60	98.03%	193	96.22%	1	
Kingsoft	0	100.00%	16	99.10%	2119	41.19%	2605	48.97%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	216	95.77%		
Microsoft	0	100.00%	0	100.00%	141	95.02%	1054	79.35%		
MWTI eScan Internet Security	0	100.00%	0	100.00%	122	96.00%	205	95.98%	1	
Norman Virus Control	0	100.00%	0	100.00%	766	78.86%	649	87.29%		
Quick Heal AntiVirus	0	100.00%	45	95.16%	977	79.25%	3450	32.42%	1	
Redstone Redprotect	0	100.00%	0	100.00%	60	98.03%	467	90.85%	1	
Rising Antivirus	0	100.00%	3	99.75%	1333	60.04%	1801	64.72%		
Sophos Endpoint Security and Control	0	100.00%	0	100.00%	154	92.75%	575	88.74%		13
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	357	93.01%		
Trustport Antivirus	0	100.00%	0	100.00%	449	92.36%	131	97.43%		2
VirusBuster for Servers	0	100.00%	2	99.93%	392	75.77%	1080	78.84%		

Detection rates were as solid as ever, and with the WildList fully covered and no false positives detected in the clean set, *Frisk* survives a few stability issues to claim another VB100 award.

F-Secure Anti-Virus for Windows Server 8.00 build 123

ItW	100.00%	**Polymorphic**	98.03%
ItW (o/a)	100.00%	**Trojans**	90.87%
Worms & bots	100.00%	**False positives**	1

F-Secure joined the ranks of those providing a special server edition for this test, but after the customary fast and easy installation process nothing seemed very different from the standard desktop product seen in recent tests. The layout of the small window is pleasantly accessible, and allowed all the required tuning to get tests tripping nicely along. Thorough scanning is an available option, and in some cases the default and, with a multiple-engine approach, the speed tests took quite a while to get through. The manufacturer advises that archive scanning on access is best left switched off.

Logging once again left much to be desired, with the HTML log files that were produced regularly appearing curtailed to the point of uselessness, mainly when a large number of infections was found by a single scan. Some careful scan management eventually produced some excellent detection figures, with no problems in the WildList. Unfortunately, however, one of the new additions to the clean test set, a harmless Perl editing tool, was mislabelled as a member of the Hupigon trojan family, thus denying *F-Secure* a VB100 this month and boding ill for the several other products that share core components.

Kaspersky Anti-Virus for Windows Server Enterprise Edition 6.0.2.551

ItW	100.00%	**Polymorphic**	98.03%
ItW (o/a)	100.00%	**Trojans**	96.22%
Worms & bots	100.00%	**False positives**	1

Kaspersky's server version installs its basics as a bare protection system with no controls made available to the general user, but instead a special administration interface is provided for admins to manage system protection remotely. Again based on the MMC, this proved reasonably easy to navigate and access to the core controls was soon established.

Stability and logging presented no problems, and detection rates were highly impressive as expected, with a concomitant sluggishness in scanning times and overheads as files were subjected to close scrutiny. Unsurprisingly, the Perl tool which tripped up *F-Secure* also produced a false positive here, and thus *Kaspersky* is denied a VB100 award this time despite full coverage of the WildList samples.

Kingsoft AntiVirus 2008.2.22.11

ItW	100.00%	**Polymorphic**	41.19%
ItW (o/a)	100.00%	**Trojans**	48.97%
Worms & bots	99.10%	**False positives**	0

Kingsoft, proud holder of a brace of VB100 awards, has had some problems with stability in recent tests, with detection rates fluctuating wildly from one install to another. No such issues were in evidence this time around however, with a pleasantly designed interface providing ample controls in an easy fashion and scanning holding strong under a heavy onslaught of infected samples.

Detection rates were markedly improved in the set of worms and bots, but still lagging somewhat elsewhere, while the WildList was handled without difficulties. In the clean sets scanning speeds were remarkably slow in both on-demand and on-access measurements, but no false positives were raised and *Kingsoft* thus earns itself a third VB100 award.

McAfee VirusScan Enterprise 8.5.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.77%
Worms & bots	100.00%	**False positives**	0

McAfee's product remains a stolid old trooper, unlovely perhaps, but efficient and businesslike with its sensible, unflashy design. Accessing the required controls proved no problem after much exposure to the same interface, and the tests were completed in excellent time, helped along by reasonable scanning speeds and an absence of any wobbliness or other unexpected behaviour.

Detection rates were excellent and reliable, and with no false positives or WildList misses *McAfee* also adds another notch to its VB100 bedpost.

Microsoft Forefront Client Security 1.5.1958.0

ItW	100.00%	**Polymorphic**	95.02%
ItW (o/a)	100.00%	**Trojans**	79.35%
Worms & bots	100.00%	**False positives**	0

Forefront, corporate big brother of *Microsoft*'s *OneCare*, has a slick and very *Windows*-y appearance, with an unsurprising but rather disappointing lack of serious configuration options. On demand at least the defaults were very thorough, with all files and all archive types scanned to an impressive depth, but nevertheless speeds were decent and tests completed in good time with no false positives to upset things.

Scanning the infected sets was similarly free from excessive difficulty, although in larger sets the product's insistence on using the event log as its only usable means of reporting caused some headaches, when large numbers of detections of a single variant tried to squeeze into a single event entry, overflowing it and losing some data. Nevertheless, results were eventually obtained, showing pretty good detection rates and complete coverage of the WildList, thus earning *Microsoft* another VB100 award.

MWTI eScan Internet Security for Windows 9.0.826.233

ItW	100.00%	**Polymorphic**	96.00%
ItW (o/a)	100.00%	**Trojans**	95.98%
Worms & bots	100.00%	**False positives**	1

MWTI's *eScan* is another product based on *Kaspersky Lab*'s *AVP* engine, and as such seemed at risk from the same minor misdemeanour which has brought a couple of products low this month. The installation was smooth, fast and simple, with an automatic scan of system areas and a reboot afterwards, and once running, the interface proved amenable, although accessing the browse function of the on-demand scanner often took rather a long time. As

Archive scanning		ACE	CAB	JAR	LZH	RAR	TGZ	ZIP	ZIP-SFX	EXT*
Agnitum Outpost	OD	X	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
AhnLab V3Net	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast!	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X
Arcabit ArcaVir	OD	2	√	√	√	√	√	√	√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	√	√
AVG	OD	X	√	X	X	√	X	√	√	X
	OA	X	X	X	X	X	X	X	X	X/√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
CA eTrust	OD	X	X/√	X/√	X/√	X/√	X/√	X/√	X	√
	OA	X	X	1	X	X	X	1	X	√
ESET NOD32	OD	√	√	√	√	√	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	√	2	√	√	√	2	2	√
F-Secure Internet Security	OD	X	5	5	5	5	2	5	5	X
	OA	X/√	X/5	X/5	X/5	X/5	X/2	X/5	X/5	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√	√
Kingsoft Internet Security	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X	X	X	X	X	X	X	X	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/9	√
Microsoft Forefront	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	1	X	X	X	1	1	√
Moon Secure	OD	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	√
MWTI eScan Internet Security	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Virus Control	OD	X	X	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	√
Quick Heal AntiVirus	OD	X/2	X/5	X/5	X	2/5	X/1	2/5	√	X
	OA	X	X	X	X	X	X	X	X	X
Redstone Redprotect	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Rising Antivirus	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Sophos Endpoint Security and Control	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	OD	X	3/√	3/√	3/√	3/√	X/3	3/√	3/√	√
	OA	X	X	X	X	X	X	X	X	√
Trustport Antivirus	OD	X	√	√	X	√	√	√	√	√
	OA	X	√	√	X	√	√	√	√	√
VirusBuster for Servers	OD	X	X	X	X	X	X	X	X	X
	OA	X	X	X	X	X	X	X	X	√

Key:

X - Archive not scanned

√ - Archives scanned to depth of 10 or more levels

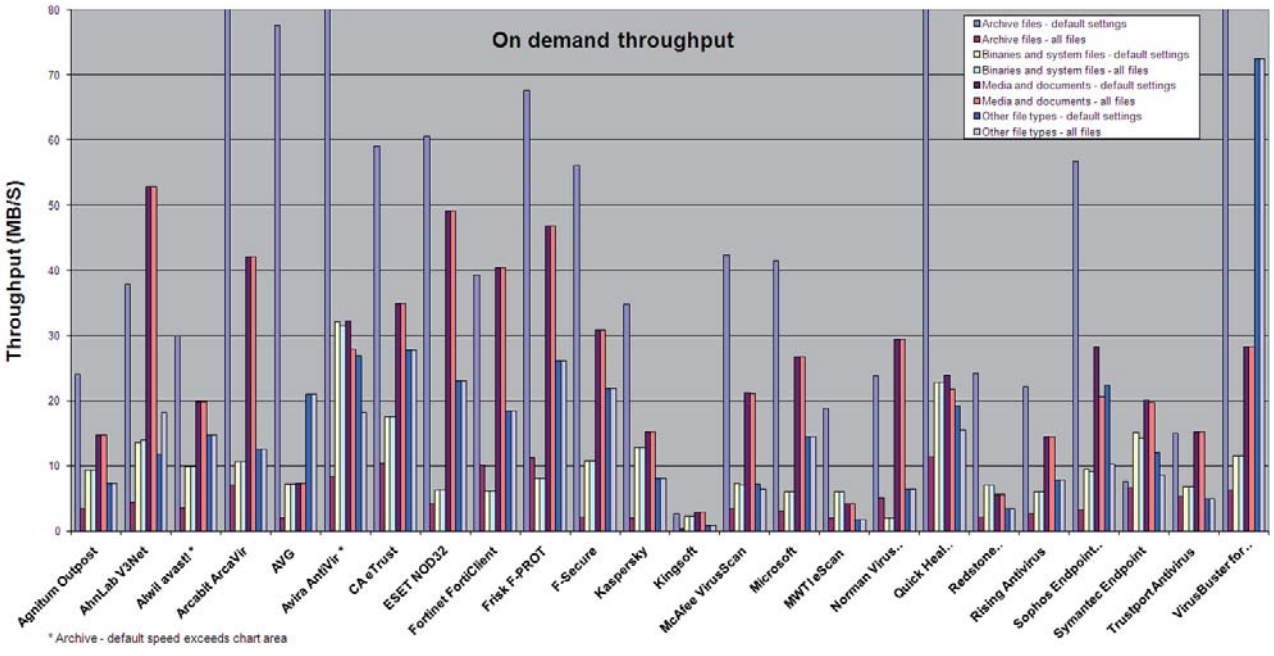
[1-9] - Archives scanned to limited depth

X/√ - Default settings/thorough settings

*Executable file with randomly chosen extension

expected, scanning speeds were less than stellar, but great thoroughness was evident in both the depth and breadth of file types scanned and in the excellent detection rates across the sets.

No problems were encountered in the WildList but, as feared, that pesky Perl utility once again popped up while scanning the clean sets, and this single false positive is enough to spoil *MWTI*'s chances of a VB100 this time.



Norman Virus Control 5.99

ItW	100.00%	**Polymorphic**	78.86%
ItW (o/a)	100.00%	**Trojans**	87.29%
Worms & bots	100.00%	**False positives**	0

After the appearance of a rather unusual new product from *Norman* in the last comparative, it came as something of a relief to see the more familiar version back once more for this test.

The product itself is not without its quirks, with on-demand scans necessitating the use of multiple windows to access configuration, scan design and actual running, but once we had refamiliarized ourselves with this things moved along nicely. Scanning extremely large infected sets proved a rather slow job, presumably as the 'sandbox' system delved deeply into malicious behaviours, but over the clean test sets speeds were splendid in some areas and at least decent in others. Detection rates were similarly reasonable, with no problems in either the WildList or the clean set, and *Norman* thus qualifies for a VB100 award.

Quick Heal AntiVirus Lite 9.50

ItW	100.00%	**Polymorphic**	79.25%
ItW (o/a)	100.00%	**Trojans**	32.42%
Worms & bots	95.16%	**False positives**	1

Quick Heal's product presents a chirpy, friendly face to the world, and continues to justify its name with rapidity in most areas. Installation was a breeze, with a complimentary pre-scan of system areas and no reboot required, and navigating the interface presented no shocks or pitfalls.

Scanning speeds were, well, quick, and overheads barely noticeable, while detection rates were only reasonable, with the trojan set particularly poorly covered. The WildList presented far fewer difficulties however, and a VB100 seemed assured, until a single item in the clean set, a component of the popular 'IrfanView' utility long lurking somewhere in the depths of the set, was mislabelled as a password-stealing trojan. As a result, no VB100 award is granted to *Quick Heal* this month.

Redstone Redprotect Anti-Virus 1.7.1.0

ItW	100.00%	**Polymorphic**	98.03%
ItW (o/a)	99.89%	**Trojans**	90.85%
Worms & bots	100.00%	**False positives**	1

Redprotect is another implementation of the *Kaspersky* scanning engine, aimed here at the managed service arena, and thus with little interaction from end-users intended. A rough engineer's interface is kindly provided to grant some access to the controls without having to resort to registry adjustments, but this was barely needed as sensible defaults were in place across the board. In an improvement on previous performances, the defaults seemed to function as expected throughout. At one point a scan was kicked

On-demand throughput	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	127	24.07	888	3.44	390	9.38	390	9.38	140	14.74	140	14.74	130	7.25	130	7.25
AhnLab V3Net	81	37.86	679	4.50	270	13.55	263	13.91	39	52.92	39	52.92	80	11.78	52	18.12
Alwil avast!	102	29.96	839	3.64	369	9.92	369	9.92	104	19.85	104	19.85	64	14.72	64	14.72
Arcabit ArcaVir	32	94.79	438	6.98	344	10.64	344	10.64	49	42.12	49	42.12	75	12.56	75	12.56
AVG	39	77.60	1450	2.11	509	7.19	509	7.19	284	7.27	284	7.27	45	20.94	45	20.94
Avira AntiVir	35	87.24	368	8.31	114	32.09	116	31.54	64	32.25	74	27.89	35	26.92	52	18.12
CA eTrust	52	59.02	294	10.40	209	17.51	209	17.51	59	34.98	59	34.98	34	27.72	34	27.72
ESET NOD32	50	60.61	734	4.16	579	6.32	579	6.32	42	49.14	42	49.14	41	22.98	41	22.98
Fortinet FortiClient	78	39.30	303	10.09	594	6.16	594	6.16	51	40.47	51	40.47	51	18.48	51	18.48
Frisk F-PROT	45	67.67	272	11.24	454	8.06	454	8.06	44	46.91	44	46.91	36	26.18	36	26.18
F-Secure	54	56.18	1383	2.21	339	10.79	339	10.79	67	30.81	67	30.81	43	21.91	43	21.91
Kaspersky	88	34.85	1489	2.05	286	12.79	286	12.79	136	15.18	136	15.18	117	8.05	117	8.05
Kingsoft	1139	2.68	7722	0.40	1574	2.32	1574	2.32	702	2.94	702	2.94	1126	0.84	1126	0.84
McAfee VirusScan	72	42.45	894	3.42	504	7.26	517	7.08	97	21.28	98	21.06	131	7.19	146	6.45
Microsoft	74	41.49	989	3.09	610	6.00	610	6.00	77	26.80	77	26.80	65	14.50	65	14.50
MWTI eScan Internet Security	162	18.87	1484	2.06	604	6.06	604	6.06	495	4.17	495	4.17	508	1.85	508	1.85
Norman Virus Control	128	23.84	600	5.09	1774	2.06	1774	2.06	70	29.48	70	29.48	147	6.41	147	6.41
Quick Heal AntiVirus	30	103.40	268	11.41	161	22.73	161	22.73	86	24.00	95	21.73	49	19.23	61	15.45
Redstone Redprotect	126	24.25	1385	2.21	522	7.01	522	7.01	363	5.69	363	5.69	269	3.50	269	3.50
Rising Antivirus	138	22.11	1125	2.72	611	5.99	611	5.99	143	14.43	143	14.43	120	7.85	120	7.85
Sophos Endpoint Security and Control	54	56.61	928	3.29	385	9.50	404	9.06	73	28.27	100	20.64	42	22.44	92	10.24
Symantec Endpoint Protection	407	7.51	459	6.66	243	15.06	258	14.18	103	20.04	105	19.66	78	12.08	110	8.57
Trustport Antivirus	204	15.01	568	5.38	537	6.81	537	6.81	136	15.18	136	15.18	190	4.96	190	4.96
VirusBuster for Servers	33	92.47	485	6.30	319	11.47	319	11.47	73	28.27	73	28.27	13	72.49	13	72.49

off with apparently no effect; while the number of files processed rocketed quickly upward, the number actually scanned and, more significantly, the number of detections, remained at zero. Restarting the job rectified things, and the issue was not repeated, but nevertheless it proved a little disquieting. Logging was also a little fiddly, with each handful of detections recorded in a separate XML file, which soon built up to an impressive number, requiring considerable processing power to draw out the required data, but with a little patience this was soon achieved.

As expected, detection results were generally excellent, and speeds more on the medium side, with again that single item in the clean set false alarmed on. Also here, a single sample in the WildList, an autorun type worm, was rather surprisingly not picked up on access, pushing a VB100 award still further from *Redstone*'s reach this month.

Rising Antivirus 2008 20.59.22

ItW	100.00%	**Polymorphic**	60.04%
ItW (o/a)	100.00%	**Trojans**	64.72%
Worms & bots	99.75%	**False positives**	0

Rising, flushed with success after achieving its first VB100 award in the last comparative review, returns to the test bench with what seems to be an identical product. The slick and smooth installer led to a similarly clear and usable interface, accompanied by a cavorting lion cartoon on the desktop, which greatly entertained the new member of the testing team with its antics.

Speeds were a little below par, and detection rates slightly on the patchy side in the polymorphic and trojan test sets, but stability was rock solid throughout the test. No problems were encountered in the WildList, and with no false positives generated either, *Rising* takes home its second VB100 in a row.

Sophos Endpoint Security and Control 7.3.5

ItW	100.00%	**Polymorphic**	92.75%
ItW (o/a)	100.00%	**Trojans**	88.74%
Worms & bots	100.00%	**False positives**	0

Sophos's core product continues a long run with no visible changes, despite much activity in the company's portfolio, and remains a pleasant midpoint between corporate sterility and cartoonish glossiness. As remarked previously, the installer offers the exciting prospect of removing competitors' products from the system before getting underway, and soon has things up and running without the need for a reboot. The initial, fairly lax settings can easily be upped to cover a more thorough range of file and archive types, with some even more in-depth configuration tucked away in a super-advanced section. Scanning moved along at a pleasant pace with no upsets or shocks.

Detection rates were mostly pretty good, and speeds decidedly so. With no problems in either the WildList or the clean set, beyond a fair number of samples flagged as using unusual packing techniques, *Sophos* is awarded a VB100.

Symantec Endpoint Protection 11.0.2020.56

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.01%
Worms & bots	100.00%	**False positives**	0

Symantec's product, once dignified and humourless, has veered to the other extreme, with a curvy, gaudy design clearly aimed at the less business-like business user. With the change has come an inevitable reduction in the wealth of options available, but the product remains generally stable and solid.

Opening large logs from within the interface brought the system to a near halt on several occasions, with several long periods of unresponsive, transparent windows to be endured before the required data could be accessed. However, once acquired and parsed, with a great deal of extraneous material discarded, results were much as expected. Speeds were reasonable on demand and very good on access, detection rates pretty high with complete coverage of the WildList, and with no false positives evident *Symantec* earns a VB100 award.

Trustport Antivirus 2.8.0.3007

ItW	100.00%	**Polymorphic**	92.36%
ItW (o/a)	100.00%	**Trojans**	97.43%
Worms & bots	100.00%	**False positives**	0

Trustport's multi-engine approach has fluctuated greatly of late, both in the range of engines available and its success in *VB* testing. Now the company seems to have settled on just two engines: those of *AVG* (here still labelled *Grisoft*, in defiance of the firm's recent name change) and *Norman*. The *AVG* engine appears to be enabled at all times, with the *Norman* engine an extra which is on by default but can be deactivated.

Aside from some strange use of English in the installation process, and some issues with the logging of outsize test sets, no major difficulties were encountered. Speeds were not the best, thanks to the doubling up of engines, but detection rates were highly praiseworthy. In the clean sets, a couple of items were highlighted as using suspicious packing techniques, in wording which came dangerously close to being adjudged false positives, but these were not in the end deemed to be full false alerts.

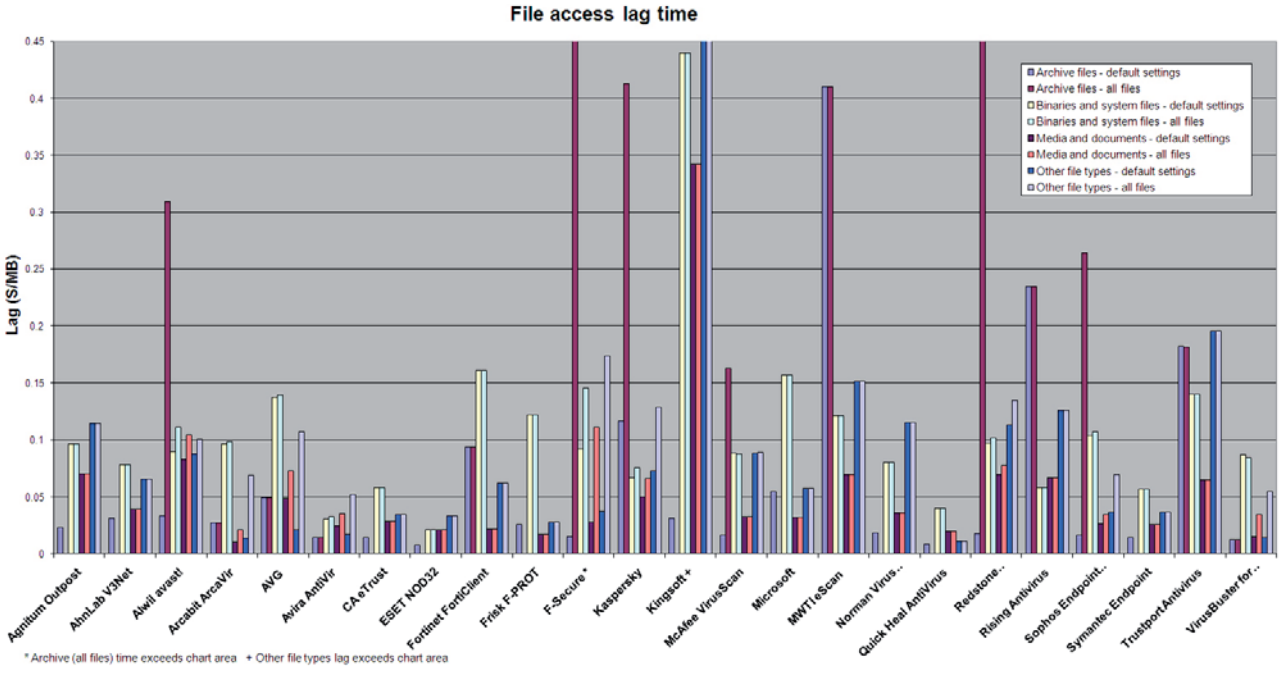
With no other problems *Trustport* scrapes through to a VB100 award after some rocky results in recent months.

File access lag time	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	73	0.02	N/A	N/A	369	0.10	369	0.10	171	0.07	171	0.07	127	0.11	127	0.11
AhnLab V3Net	97	0.03	N/A	N/A	303	0.08	303	0.08	108	0.04	108	0.04	81	0.07	81	0.07
Alwil avast!	103	0.03	948	0.31	346	0.09	424	0.11	197	0.08	242	0.10	102	0.09	114	0.10
Arcabit ArcaVir	85	0.03	85	0.03	370	0.10	377	0.10	48	0.01	69	0.02	32	0.01	84	0.07
AVG	154	0.05	154	0.05	521	0.14	528	0.14	126	0.05	177	0.07	39	0.02	120	0.11
Avira AntiVir	48	0.01	48	0.01	128	0.03	134	0.03	76	0.02	99	0.04	35	0.02	69	0.05
CA eTrust	47	0.01	N/A	N/A	228	0.06	228	0.06	85	0.03	85	0.03	52	0.03	52	0.03
ESET NOD32	25	0.01	N/A	N/A	94	0.02	94	0.02	70	0.02	70	0.02	50	0.03	50	0.03
Fortinet FortiClient	290	0.09	290	0.09	606	0.16	606	0.16	71	0.02	71	0.02	78	0.06	78	0.06
Frisk F-PROT	81	0.03	N/A	N/A	463	0.12	463	0.12	62	0.02	62	0.02	45	0.03	45	0.03
F-Secure	48	0.01	1630	0.53	354	0.09	548	0.15	84	0.03	255	0.11	54	0.04	183	0.17
Kaspersky	360	0.12	1265	0.41	261	0.07	292	0.08	129	0.05	162	0.07	88	0.07	141	0.13
Kingsoft	98	0.03	N/A	N/A	1626	0.44		0.44	733	0.34	733	0.34	1139	1.19	1139	1.19
McAfee VirusScan	53	0.02	501	0.16	340	0.09	338	0.09	93	0.03	93	0.03	102	0.09	103	0.09
Microsoft	169	0.05	N/A	N/A	590	0.16	590	0.16	92	0.03	92	0.03	74	0.06	74	0.06
MWTI eScan Internet Security	1258	0.41	1258	0.41	460	0.12	460	0.12	170	0.07	170	0.07	162	0.15	162	0.15
Norman Virus Control	60	0.02	N/A	N/A	311	0.08	311	0.08	100	0.04	100	0.04	128	0.12	128	0.12
Quick Heal AntiVirus	27	0.01	N/A	N/A	163	0.04	163	0.04	66	0.02	66	0.02	30	0.01	30	0.01
Redstone Redprotect	56	0.02	1390	0.45	372	0.10	390	0.10	170	0.07	187	0.08	126	0.11	147	0.13
Rising Antivirus	719	0.23	719	0.23	229	0.06	229	0.06	164	0.07	164	0.07	138	0.13	138	0.13
Sophos Endpoint Security and Control	54	0.02	811	0.26	397	0.10	410	0.11	80	0.03	97	0.03	54	0.04	85	0.07
Symantec Endpoint Protection	46	0.01	N/A	N/A	223	0.06	223	0.06	79	0.03	79	0.03	54	0.04	54	0.04
Trustport Antivirus	558	0.18	558	0.18	529	0.14	529	0.14	160	0.06	160	0.06	204	0.20	204	0.20
VirusBuster for Servers	41	0.01	41	0.01	334	0.09	324	0.08	56	0.01	97	0.03	33	0.01	71	0.05

VirusBuster for Servers 6.0 build 205

ItW	100.00%	**Polymorphic**	75.77%
ItW (o/a)	100.00%	**Trojans**	78.84%
Worms & bots	99.93%	**False positives**	0

VirusBuster brings up the rear of the test as usual, with much the same product as seen in numerous previous tests and few explicit nods to the server environment. The layout is somewhat esoteric and fiddly, and was not popular with the new member of the team, who was tasked with tackling its strange design to set up a series of scheduled scans over



a long weekend, but once the right technique was hit upon testing was completed tolerably easily, with no serious problems.

Scanning speeds were pretty impressive, quite startlingly so in scanning miscellaneous file types on demand, but on access the option to enable archive scanning seemed not to function as promised. Detection rates were mostly reasonable, though not so hot in the trojan set, but with no false positives or WildList misses *VirusBuster* completes this comparative on a high, winning a VB100 award.

CONCLUSIONS

Another month, another comparative review, this one rendered rather special by the new additional help available in the testing lab, which enabled the review to squeeze in under the wire just before the team heads off to Ottawa for this year's *VB* conference. It was a pretty close call however, with many products taking far longer to get through the test than expected, mainly due to instability under heavy pressure and unexpected, even downright contrary behaviour.

The instability and bad behaviour was most in evidence in the additional testing running parallel with this month's test, trialling a new setup we hope to have fully operational soon. The trial has shown some serious difficulties with persuading some products to behave themselves properly when called on to do their very utmost, meaning that some minor tweaks to the test design may be required prior to the official introduction of these tests, in order to ensure useful data can be obtained and presented in a reasonable time frame.

In the main body of the test, things were much as usual. A few products had some issues with the WildList, with the very pesky W32/Virut#10 once again raising its ugly head after many months on the list. The main reason for products being denied certification, however, was the generation of false positives, with only a handful of files tripping up a sizeable number of products. This was mostly thanks to several products including the same single engine, which in turn mislabelled a single file. This is an indicator of the toughness and the unforgiving nature of the VB100 system, and what makes it such a sought-after and widely respected scheme. Those products that managed to pass should hold their heads up high, while those who didn't quite make it this time, all highly regarded and reliable products, will likely find themselves back up on the podium soon.

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 Server 2008* (32-bit).

Any developers interested in submitting products for VB's comparative reviews should contact john.hawes@virusbtn.com. The current schedule for the publication of VB comparative reviews can be found at http://www.virusbtn.com/vb100/about/schedule.xml.