COMPARATIVE REVIEW

WINDOWS SERVER 2008 STANDARD EDITION SP2 X86

John Hawes

Our second visit to *Microsoft*'s *Server 2008* platform could also be our last in its current incarnation, with the imminent and much anticipated release of *Windows 7* now just a few weeks away. While *Vista*, which seems doomed to fade into history with the early arrival of a replacement, will not be missed by most users (even those who have got around to adopting it), the server edition that accompanied it has proved a much finer package, easily eclipsing the earlier *2003 Server* in terms of speed, stability and general likeability. Looking forward, we hope the R2 edition will produce more of the same, and we will monitor its uptake among users before deciding whether to cease testing on the original version.

With the annual *VB* conference taking the whole team out of the lab for a full week in the middle of testing this month, we knew in advance that timing would be a major issue, and with the ever-growing numbers of products entering our desktop tests it was clear that running a less well-subscribed server test would be the only way to survive the month. As it was, the test still proved popular, with some 26 products making the final cut on the deadline day.

PLATFORM AND TEST SETS

Setting up the test systems is by now fairly routine, with the application of a service pack to existing images not taking too much time or effort. As mentioned, the platform offers a much less frustrating user experience than its desktop sibling *Vista*, with all the required tools fairly close at hand. One step we did take to simplify matters was to disable the UAC system, assuming that an administrator operating his own server would know his business and would not want to be interrupted by intrusive pop-ups during software set-up. After having experienced some serious problems with system crashes in the recent *Vista* test (see *VB*, August 2009, p.14), we ran a few tests on the hardware to ensure there were no problems, and planned to watch out for any repetition of the worrying trend during the weeks ahead.

The deadline for product submissions was set for 26 August. Test sets were aligned with the July issue of the WildList and standard sets, including the clean sets, were frozen on 22 August. Of course, we continued collecting samples for a further week after the product submission deadline to complete our RAP sets.

In the WildList set there were few items of interest – a smattering of the usual suspects mostly targeting online gamers and social networkers – but a couple of variants of W32/Virut, both added more recently than the one which caused some upsets in the last comparative, looked likely to produce some difficulties of their own. Voraciously infectious and demonstrating highly complex polymorphism, they seemed certain to provide a stiff challenge to the detection capabilities of the products under test, and were added to our set in large numbers to provide a good measure of how thoroughly detection had been implemented.

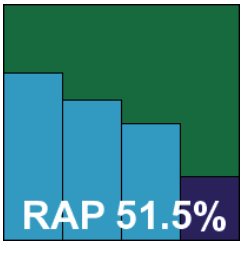
Elsewhere there were few changes beyond some further expansion of some of the other Virut strains recently relegated to the polymorphic test set. A minor update was made to our clean sets, with no obscure or unusual samples likely to trip any heuristics. The speed sets did see something of an overhaul, following up on some of the housecleaning done on the clean sets in recent months, with a fair number of older and rarer samples removed and replaced with more recent samples from major software providers. As this set is designed to measure speed only, we do our best to avoid including any files which are likely to cause false alarms, but nevertheless the occasional product will skew its speed figures by alerting on something in here and the set is officially included as part of our false positive test. Further updates to the speed testing system, along with ongoing overhauls of other areas, should, we hope, be in place in time for the next comparative.

With everything set up for the test, we got to work ploughing through the field of products with only a couple of weeks in which to get the bulk of testing out of the way, putting a great deal of trust in the stability of the platform to minimize the impact of any bad behaviour on the part of the products.

AhnLab V3Net for Windows Servers 7.0.2.2 build 963

ItW	99.99%	**Polymorphic**	99.56%
ItW (o/a)	99.99%	**Trojans**	75.83%
Worms & bots	99.79%	**False positives**	0

AhnLab's server-oriented product seems fairly similar to the desktop range commented on in the last review (see *VB*, August 2009, p.14), with a nice speedy installation and a fairly pleasant-looking interface. This similarity extended to a relative shortage of configuration options,

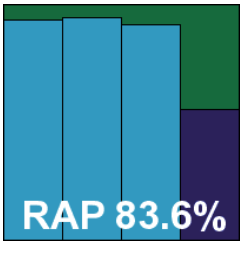


which many server administrators may find inadequate for their needs. We also found the splitting of scanning and detections into separate sections headed 'virus' and 'spyware' not only rather senseless in this modern age of boundary-stretching threats, but also somewhat confusing and on occasion dangerous. As noted before, while the on-access protection blocked most items on our list, some seemed to be spotted first by the spyware side, which meant that blocking was not implemented. With the spyware module disabled, protection from more serious threats actually seems to improve.

With these initial frustrations worked out, running through the tests went fairly smoothly with no repeat of the problems with logging and crashes noted in the last comparative. Scanning speeds were fairly reasonable, looking better on access thanks to the highly limited selection of files actually scannable, and detection rates seemed fairly decent too, with levels dropping in fairly steep steps throughout the RAP sets. Despite all looking good in the clean sets, a fair number of samples of one of the W32/Virut strains on the WildList were not detected, and *AhnLab* thus misses out on a VB100 this month.

Alwil avast! Professional 4.8.1099

ItW	100.00%	**Polymorphic**	99.32%
ItW (o/a)	100.00%	**Trojans**	94.99%
Worms & bots	99.96%	**False positives**	0

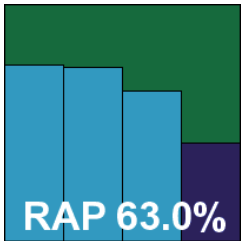


Alwil's product is another that looks and feels identical to the desktop edition, and again comes with its own selection of oddities and idiosyncrasies of design and layout; a new version, believed to be on the verge of release, is hotly anticipated. Navigating the rather complex process of designing scan tasks, and monitoring them through a system which seems to refresh irregularly and not always very cleanly, is not a great problem though, and a full set of configuration should allow even the most demanding of admins to protect their servers in any manner desired.

Scanning speeds were excellent, even with more thorough settings selected, and detection rates pretty superb too, with a very commendable average achieved in the RAP test despite a fair sized drop in the week +1 set. False positives were entirely absent, and misses absent from the WildList set, thus setting *Alwil* on course to take the first VB100 award of this month's comparative.

Authentium Command Anti-Malware 5.0.8

ItW	99.99%	**Polymorphic**	99.65%
ItW (o/a)	99.99%	**Trojans**	66.42%
Worms & bots	100.00%	**False positives**	0



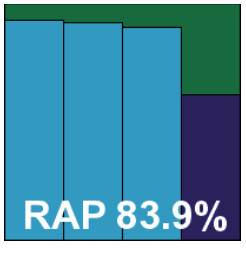
Authentium's *Command* product is a semi-regular entrant in our comparatives, and only decided at the last minute to join this one, but is always welcome thanks to simple design and stable behaviour. The interface, unchanged from its last appearance, is pared down in the extreme, but still provides a few basic options, most of which require the 'advanced' option to be selected before they can be accessed. A couple of items which did slow down the test this month were a lack of information on the logging and archive handling, which is all in place but a little vague, and the apparent failure of the scheduler to fire up the scans we diligently prepared to run overnight.

Nevertheless, the tests were soon completed. Scanning speeds were around the mid range, with on-access overheads perhaps a little heavier than expected. Detection rates were decent too, somewhat improved over recent performances and surprisingly doing slightly better in the reactive part of the RAP sets than in the older samples in the trojans set. All looked pretty good, but in the WildList set those large collections of W32/Virut variants took another victim, with around 10% of samples of the most recent strain missed. *Authentium* thus does not quite make the cut for a VB100 award this time.

AVG Internet Security Network Edition 8.5.409

ItW	100.00%	**Polymorphic**	99.06%
ItW (o/a)	100.00%	**Trojans**	93.57%
Worms & bots	99.96%	**False positives**	0

AVG opted to enter a standard desktop suite, although this time it was a business-oriented version compatible with remote administration tools. Installation was simple, fast and easy, with no reboot required, and on the surface the control centre looks much as



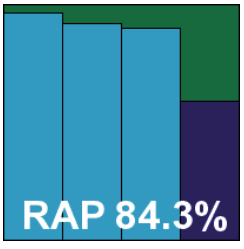
On-demand detection	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets
	Missed	%	Missed	%	Missed	%	Missed	%	FP
AhnLab V3Net	171	99.99%	5	99.79%	24	99.56%	3167	75.83%	0
Alwil avast!	0	100.00%	1	99.96%	7	99.32%	656	94.99%	0
Authentium Command	159	99.99%	0	100.00%	15	99.65%	4400	66.42%	0
AVG I.S. Network Edition	0	100.00%	1	99.96%	25	99.06%	843	93.57%	0
Avira AntiVir Server	1	99.99997%	0	100.00%	0	100.00%	162	98.76%	0
BitDefender Security	0	100.00%	0	100.00%	0	100.00%	2244	82.87%	0
CA eTrust	0	100.00%	0	100.00%	1750	92.34%	8079	38.35%	0
eScan Internet Security	0	100.00%	1	99.96%	0	100.00%	2202	83.19%	0
ESET NOD32	0	100.00%	0	100.00%	2	99.998%	968	92.61%	0
Filseclab Twister	5655	95.54%	354	85.29%	10001	33.69%	5213	60.22%	1
Fortinet FortiClient	38	99.999%	0	100.00%	4	99.70%	2403	81.66%	0
Frisk F-PROT	159	99.99%	0	100.00%	12	99.78%	4291	67.25%	0
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1165	91.11%	0
G Data AntiVirus	0	100.00%	0	100.00%	0	100.00%	228	98.25%	0
Ikarus virus.utilities	3759	99.87%	3	99.88%	5754	73.93%	191	98.54%	4
K7 Total Security	0	100.00%	0	100.00%	0	100.00%	1822	86.09%	0
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1278	90.24%	0
Kingsoft I.S. 2009 Advanced	98	99.996%	10	99.58%	3282	61.94%	10327	21.20%	0
Kingsoft I.S. 2009 Standard	2461	99.91%	11	99.54%	4572	59.94%	12161	7.20%	0
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	1229	90.62%	0
Microsoft Forefront	0	100.00%	0	100.00%	0	100.00%	973	92.57%	0
Quick Heal AntiVirus Lite	0	100.00%	3	99.88%	150	98.28%	2436	81.41%	0
Sophos Anti-Virus	1	99.99997%	0	100.00%	0	100.00%	1231	90.60%	0
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	1031	92.13%	0
Trustport Antivirus 2009	0	100.00%	0	100.00%	0	100.00%	265	97.97%	0
VirusBuster for Servers	5	99.9998%	2	99.92%	193	90.43%	2631	79.92%	0

we have come to expect lately: smooth and professional, with an abundance of icons leading to various protective modules. The layout is easy to navigate and provides a reasonable if not quite exhaustive level of configuration, and testing ran smoothly and without issues.

Scanning speeds were reasonable in both modes across the speed sets, although our heavily enlarged clean set with many multi-layered archives did take some time to trawl through, and in the infected sets detection rates were pretty excellent across the board, with a superb showing in the RAP sets. With no issues with false alarms or in the WildList, *AVG* comfortably takes home a VB100 award.

Avira AntiVir Server 9.00.00.25

ItW	99.99%	**Polymorphic**	100.00%
ItW (o/a)	99.99%	**Trojans**	98.76%
Worms & bots	100.00%	**False positives**	0

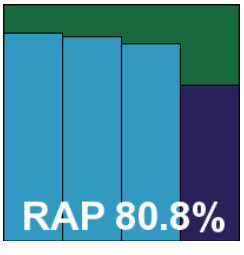


The first proper server version on offer this month, *Avira*'s product uses the standard MMC system to provide access to its controls, which seem fairly thorough once the layout has been deciphered. Options to exclude handling of selected *Windows* services seemed an especially appropriate addition for a server product. The setting up and running of scans required a little further investigation into the GUI design, and the monitoring of progress even more exploring, but scanning speeds made up for lost time with some decent speeds, perhaps not up to the usual excellent levels but quite acceptable. Some initial runs over the infected sets turned up a malformed file which seemed to cause the scanner some problems, shutting down the scan on several occasions and at one point apparently disabling the on-access scanner, although this effect could not be reproduced.

As in many recent tests, detection rates were quite remarkable throughout, with no false alarms despite the high detection rate. In the WildList however, a single item from one of the large sets of Virut samples was not detected. We retried the product over an even larger set generated during testing, and were able to find a further small handful of such samples to provide to the vendor for analysis. The incidence of missed samples was so low that we have had to expand the score table to fit in the required number of decimal places. Nevertheless, the rules of the VB100 are strict and this single miss is enough to deny *Avira* a VB100 award this month despite an otherwise superb performance.

BitDefender Security for Windows Servers 3.3.54

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	82.87%
Worms & bots	100.00%	**False positives**	0

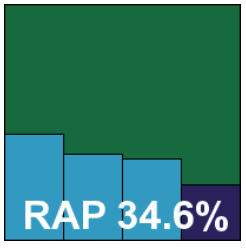


BitDefender's offering is another proper server product, again using the MMC system and again finding it difficult to squeeze all the required controls and displays in without compromising usability somewhat. After a simple but rather sluggish installation, the interface presents a few challenges in navigation, lacking the smooth slickness of the desktop range, but once a few familiar paths have been uncovered it responds well and the whole solution runs in a stable, well-behaved manner.

Scanning speeds and overheads were fairly average, but detection levels were strong, with a solid showing in the proactive part of the RAP sets pushing the product's score up to a very respectable level. With no issues with any of the nasty polymorphic samples in the WildList or elsewhere, and no false alarms, *BitDefender* earns a VB100 award.

CA eTrust 8.1.655.0

ItW	100.00%	**Polymorphic**	92.34%
ItW (o/a)	100.00%	**Trojans**	38.35%
Worms & bots	100.00%	**False positives**	0



CA's business line continues with the same product as seen in many previous tests – however, some early peeks at an updated range point to a few changes yet to come as the company's partnership with *HCL* begins to show some signs of blossoming. The install is as ever lengthy, with a plethora of EULAs to agree to and a full page of personal data to fill in. Once up and running, response times were much better than they tend to be on *XP*, which made navigating the interface somewhat more pleasant, but as usual results are better ripped from raw logging data than viewed in the interface.

Scanning speeds remain hard to beat, although full measurements were not taken as the option to enable archive scanning on access, although present in the interface, remains non-functional. Detection rates seemed perhaps slightly improved compared to recent showings. This leaves a fair way to go, but the WildList and clean sets were handled ably and *CA* thus earns another VB100 award.

eScan Internet Security 10.0.997.514

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	83.19%
Worms & bots	99.96%	**False positives**	0

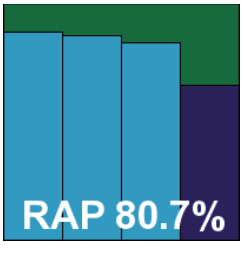
The people behind *eScan* have opted to remove their company name from promotion, so the results formerly listed under *MicroWorld* (and occasionally *MWTI*) will henceforth be referred to, more simply and more memorably, as *eScan*. The product is unchanged however,

On-access detection	WildList		Worms & bots		Polymorphic viruses		Trojans		Clean sets
	Missed	%	Missed	%	Missed	%	Missed	%	FP
AhnLab V3Net	171	99.99%	9	99.63%	24	99.56%	3356	74.39%	0
Alwil avast!	0	100.00%	1	99.96%	7	99.32%	656	94.99%	0
Authentium Command	159	99.99%	0	100.00%	15	99.65%	4587	65.00%	0
AVG I.S. Network Edition	0	100.00%	1	99.96%	25	99.06%	1084	91.72%	0
Avira AntiVir Server	1	99.99997%	0	100.00%	0	100.00%	162	98.76%	0
BitDefender Security	0	100.00%	0	100.00%	0	100.00%	2335	82.18%	0
CA eTrust	0	100.00%	0	100.00%	1750	92.34%	8079	38.35%	0
eScan Internet Security	0	100.00%	4	99.83%	0	100.00%	2207	83.16%	0
ESET NOD32	0	100.00%	0	100.00%	4	99.995%	840	93.58%	0
Filseclab Twister	5655	95.54%	384	84.05%	10001	33.69%	5526	57.83%	1
Fortinet FortiClient	38	99.999%	0	100.00%	4	99.70%	2404	81.65%	0
Frisk F-PROT	159	99.99%	0	100.00%	12	99.78%	4468	65.90%	0
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1677	87.20%	0
G Data AntiVirus	0	100.00%	0	100.00%	0	100.00%	228	98.25%	0
Ikarus virus.utilities	3759	99.87%	3	99.88%	5754	73.93%	191	98.54%	4
K7 Total Security	0	100.00%	0	100.00%	0	100.00%	2013	84.63%	0
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	1386	89.42%	0
Kingsoft I.S. 2009 Advanced	98	99.996%	10	99.58%	3282	61.94%	10397	20.66%	0
Kingsoft I.S. 2009 Standard	2461	99.91%	11	99.54%	4572	59.94%	12216	6.79%	0
McAfee VirusScan Enterprise	0	100.00%	0	100.00%	0	100.00%	1231	90.60%	0
Microsoft Forefront	0	100.00%	0	100.00%	0	100.00%	973	92.57%	0
Quick Heal AntiVirus Lite	0	100.00%	6	99.75%	179	96.10%	5412	58.70%	0
Sophos Anti-Virus	1	99.99997%	0	100.00%	0	100.00%	1231	90.60%	0
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	1068	91.85%	0
Trustport Antivirus 2009	0	100.00%	0	100.00%	0	100.00%	418	96.81%	0
VirusBuster for Servers	5	99.9998%	2	99.92%	193	90.43%	2631	79.92%	0

and has its usual simple and straightforward install and set-up process. Towards the end of installation we received a warning that a component had crashed, but this seemed to affect neither the install process nor the operation of the product. The interface is clean and unfussy, providing all the controls required.

The default setting limits scanning to files under 5MB, which helped us get through our large clean sets containing a number of big, deep archives and installer packages which can slow down more thorough scanners such as this.

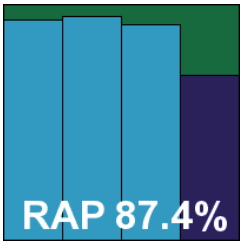
Nevertheless, the clean set took some time to get through, and the standard speed tests showed some fairly sluggish



speeds and hefty overheads. On a more positive note, detection rates continued to impress. The WildList, and indeed all the polymorphic samples tested, were handled without difficulty and no false alarms were raised in the clean set, thus earning *eScan* another VB100 award for its efforts.

ESET NOD32 Antivirus 4.0.437.0

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	92.61%
Worms & bots	100.00%	**False positives**	0



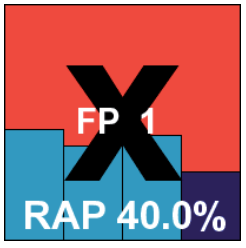
ESET's product has a rapid and simple install process which comes to a halt on the question of handling 'potentially unwanted' items, a selection which has no default and requires some actual consideration from the user – reminding us that our procedures may need some adjustment to cope with such advanced thinking. With that minor hurdle quickly overcome, we soon had access to the interface, which remains extremely slick, stylish and attractive, and manages to combine ease of use with pretty thorough levels of configurability. A few features may require a little familiarity to find, while others, such as on-access archive handling, are absent, but in general all seems to be on hand.

Scanning speeds over the clean sets were no more than a slow average, and with several levels of on-access scanning affecting different access methods we were obliged to run the test by copying sets to the system, which took quite some time and on one occasion was interrupted by the system halting unexpectedly during the night.

When we finally got some figures down they showed some excellent detection rates, with commendably even scores across the trojans and the reactive parts of the RAP set indicating steady handling of new samples, and a splendid showing in the proactive set making for a very high overall average. A tiny number of samples from some older Virut variants were missed in the polymorphic set, but the newer ones on the official WildList were handled without issues. With no false positives *ESET* is the worthy winner of yet another VB100 award, thus maintaining *NOD32*'s position as the product with the largest number of VB100 awards.

Filseclab Twister AntiVirus 7.3.2.9971

ItW	95.54%	**Polymorphic**	33.69%
ItW (o/a)	95.54%	**Trojans**	60.22%
Worms & bots	85.29%	**False positives**	1



Filseclab bravely returns for another run in the VB100, having shown gradual improvements over its first few attempts. The install process remains simple and very speedy, although it does require a reboot to complete. The main interface is quite appealing, and a decent degree of configuration is tucked away underneath, albeit in slightly less stylish settings. The product also includes a range of other features beyond standard anti-malware, including a HIPS set-up, which is really its main strength, and also a 'Fix Windows' area which tweaks and adjusts a number of settings, putting the system into a safer state either after an infection or simply on spotting some of the notoriously insecure defaults in most *Windows* versions.

On-demand scanning speeds were fairly modest, and on-access protection is implemented in a rather unconventional manner, with no instant blocking of files but alerts, actions and log entries appearing soon after an infected file is accessed. This makes our standard on-access speed measurement somewhat unreliable, but as some slowdown was observed despite the lack of file access interception we opted to record it out of interest. Detection rates still lag behind somewhat, but seem to be improving, with only a single false alert generated in the much-expanded clean set. In the WildList, a fair number of recent items were not properly handled, with fairly large swathes of both Virut strains missed too, and *Filseclab* will have to keep working its way towards a VB100 award.

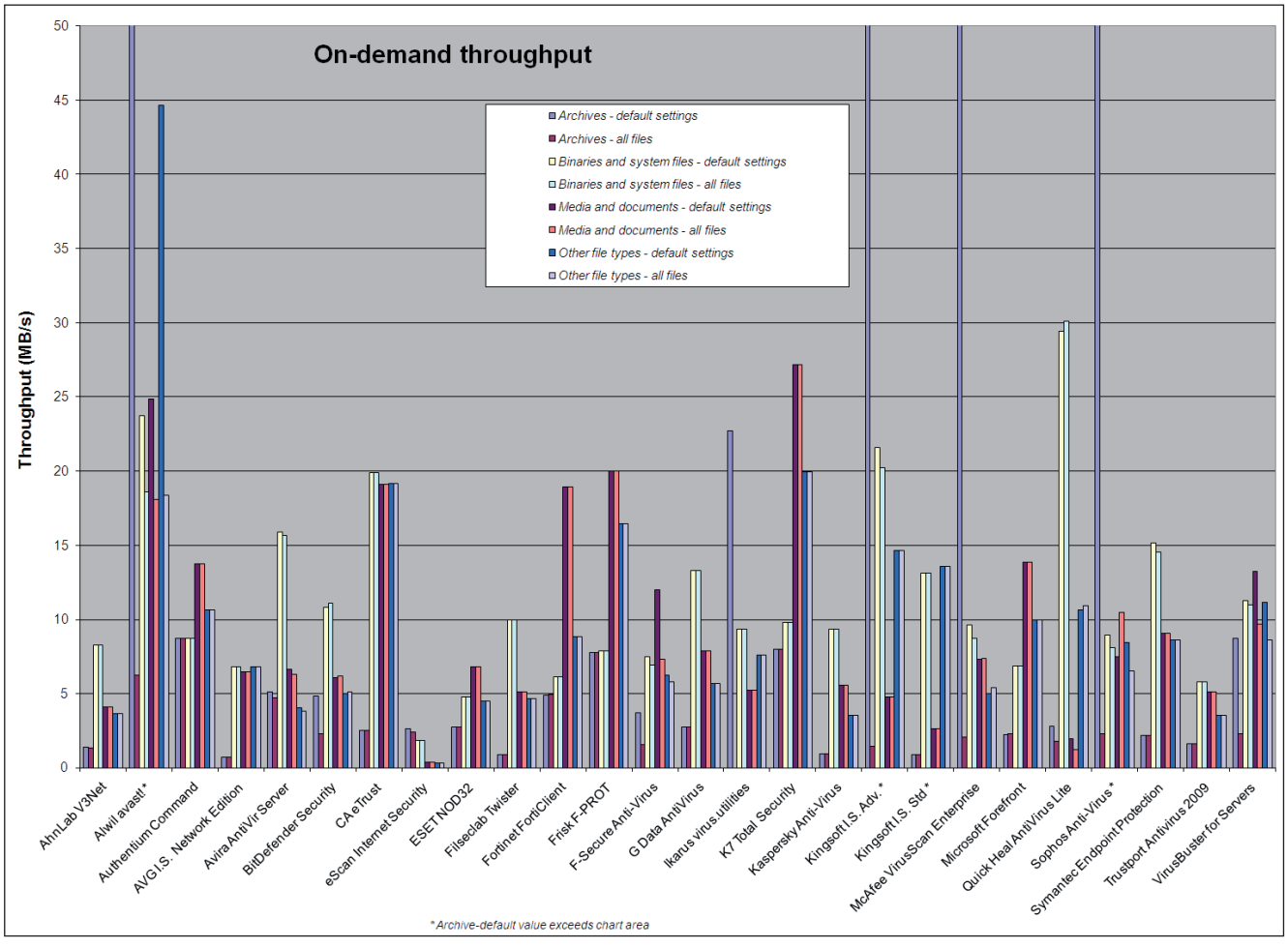
Fortinet FortiClient Endpoint Security 4.0.1.54

ItW	99.99%	**Polymorphic**	99.70%
ItW (o/a)	99.99%	**Trojans**	81.66%
Worms & bots	100.00%	**False positives**	0

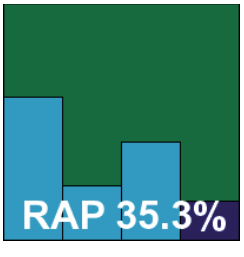
Fortinet's install process is slowed by some warning pop-ups from *Windows*, most of which can be suppressed by instructing the system to 'always trust' *Fortinet* as a software provider; it seems likely that more pop-ups would be evident were the UAC system active. Once up and running though, the product looks good and runs well.

Archive scanning		ACE	CAB	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
AhnLab V3Net I.S.	Default	9/√	9/√	9/√	9/√	9/√	9/√	X	9/√	√
	All	X	X	X	X	X	X	X	X	X
Alwil avast!	Default	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	X/√
	All	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	√
Authentium Command	Default	X	5	5	5	√	5	2	5	√
	All	X	X/4	X/4	X/4	X/√	X/4	X/2	X/4	X/√
AVG I.S. Network Edition	Default	X	√	√	√	√	√	√	√	X
	All	X	X	X	X	X	X	X	X	√
Avira AntiVir Server	Default	√	√	√	√	√	√	√	√	√
	All	X	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
BitDefender Security	Default	√	√	8	√	√	√	8	√	√
	All	X/√	X/√	√	X/√	X/√	X/√	X/√	X/√	X/√
CA eTrust	Default	X	√	X	√	√	√	√	√	√
	All	X	X	X	1	X	X	X	1	√
eScan Internet Security	Default	√	√	8	√	√	√	8	√	√
	All	X/√	X/√	X/8	X/√	X/√	X/√	X/8	X/√	√
ESET NOD32	Default	√	√	√	√	√	√	5	√	√
	All	X	X	X	X	X	X	X	X	√
Filseclab Twister	Default	5	3	3	4	1	4	X	5	√
	All	X	X	X	X	X	1	X	2	X
Fortinet FortiClient	Default	X/√	√	√	√	√	√	√	4	√
	All	X/√	√	√	√	√	√	√	4	√
Frisk F-PROT Antivirus	Default	√	√	√	√	√	√	√	√	√
	All	X	X	2	2	X	X	X	2	√
F-Secure Anti-Virus	Default	X/√	√	√	√	√	√	√	√	X/√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
G Data AntiVirus	Default	√	√	√	√	√	√	√	√	√
	All	√	√	4	√	√	√	7	8	√
Ikarus virus.utilities	Default	2	2	2	2	2	2	3	2	√
	All	2	2	2	2	2	2	3	2	√
K7 Total Security	Default	√	√	√	√	√	√	√	√	√
	All	1	X	1	1	X	X	X	1	√
Kaspersky Anti-Virus	Default	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Kingsoft I.S. 2009 Advanced	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
Kingsoft I.S. 2009 Standard	Default	√	√	√	√	√	√	√	√	√
	All	X	X	X	X	X	X	X	X	√
McAfee VirusScan Enterprise	Default	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	All	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Microsoft Forefront	Default	√	√	√	√	√	√	√	√	√
	All	X	X	1	X	X	X	X	1	√
Quick Heal AntiVirus Lite	Default	X/2	X/5	X	2/5	X	2/5	X/1	2/5	X/√
	All	X	X	X	X	X	X	X	X	X
Sophos Anti-Virus	Default	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	All	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	Default	X	3/√	3/√	3/√	3/√	3/√	X/5	3/√	√
	All	X	X	X	X	X	X	X	X	√
Trustport Antivirus	Default	√	√	√	√	√	√	√	√	√
	All	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	√
VirusBuster for Servers	Default	2	√	√	X/√	X	√	√	√	X/√
	All	X	X	X	X	X	X	X	X	X/√

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



A logical layout provides easy access to a very satisfactory range of options, quite suited to the business audience the firm targets.



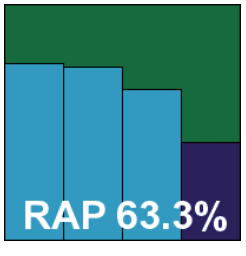
Scanning speeds were pretty decent and overheads low, and detection rates showed considerable improvement over recent tests as more of the product's optional 'extended databases' seem to have been moved to the default set-up – we noted a further jump in detection when these full databases were activated. RAP scores were somewhat uneven, and here the increased detection from the extended data was particularly significant.

No problems were found in the clean set, but in the WildList a small handful of samples of one of the Virut strains were not detected. Although we were able to generate further undetected samples to provide to the vendor fairly easily, the company's own research produced no more from batches in the tens of thousands of samples, indicating that the issue only affects a very small proportion of potential infections. Nevertheless, the misses are considered enough to deny *Fortinet* a VB100 award this month.

Frisk F-PROT Antivirus 6.0.9.3

ItW	99.99%	**Polymorphic**	99.78%
ItW (o/a)	99.99%	**Trojans**	67.25%
Worms & bots	100.00%	**False positives**	0

F-PROT has a fairly speedy install process, although we found the phrasing of the licensing page somewhat confusing, and a reboot is required to complete. The interface remains minimalist in the extreme, with very little by way of configuration and some of what

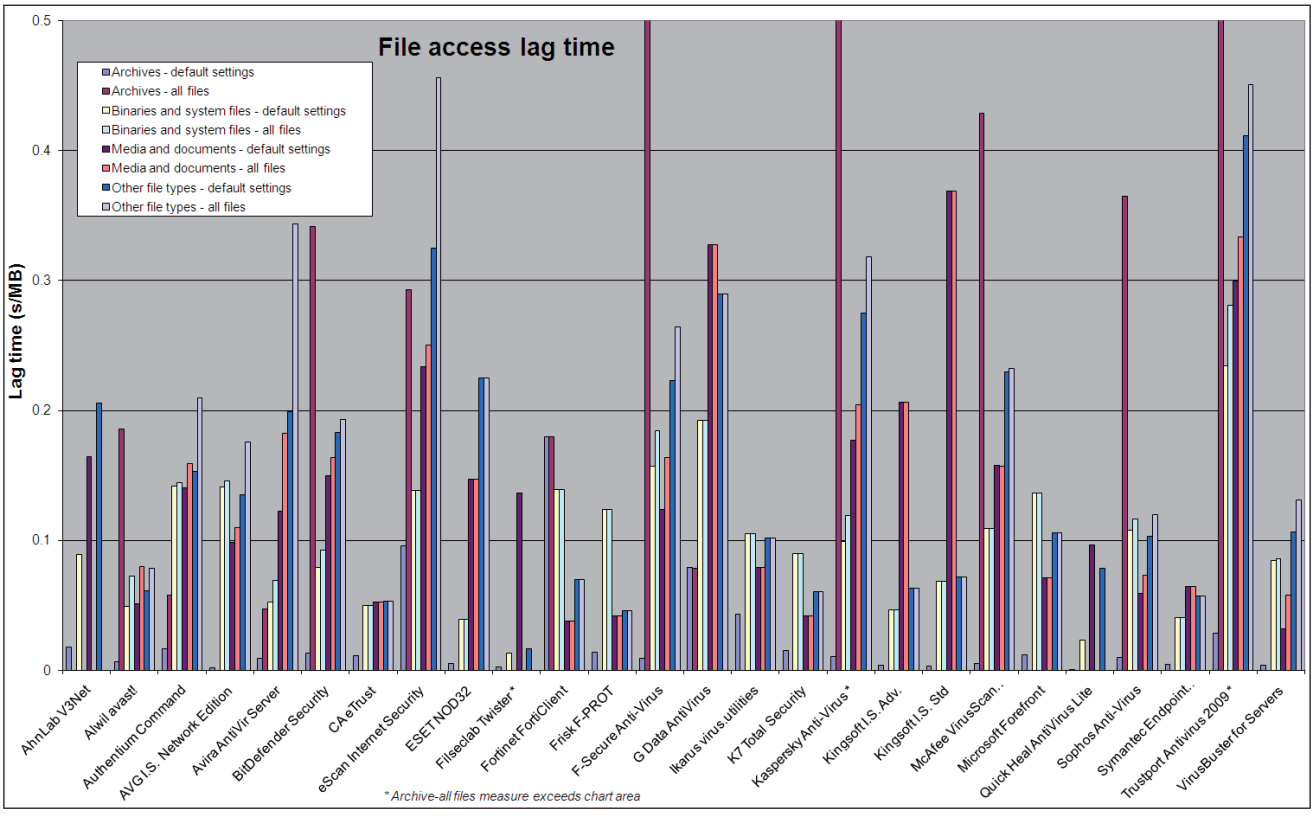


On-demand throughput (Time = s; Throughput = MB/s)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put	Time	Thr. put
AhnLab	2138	1.41	2186	1.37	312	8.30	312	8.30	501	4.12	501	4.12	258	3.64	258	3.64
Alwil	12	250.40	481	6.25	109	23.76	139	18.63	83	24.87	114	18.10	21	44.67	51	18.39
Authentium	343	8.76	343	8.76	297	8.72	297	8.72	150	13.76	150	13.76	88	10.66	88	10.66
AVG	4255	0.71	4255	0.71	381	6.80	381	6.80	318	6.49	318	6.49	138	6.80	138	6.80
Avira	585	5.14	635	4.73	163	15.89	165	15.69	309	6.68	328	6.29	231	4.06	245	3.83
BitDefender	619	4.85	1302	2.31	239	10.83	233	11.11	340	6.07	334	6.18	186	5.04	182	5.15
CA	1177	2.55	1177	2.55	130	19.92	130	19.92	108	19.11	108	19.11	49	19.14	49	19.14
eScan	1129	2.66	1254	2.40	1404	1.84	1408	1.84	4936	0.42	4936	0.42	2879	0.33	2879	0.33
ESET	1084	2.77	1084	2.77	543	4.77	543	4.77	302	6.83	302	6.83	208	4.51	208	4.51
Filseclab	3330	0.90	3330	0.90	259	10.00	259	10.00	401	5.15	401	5.15	201	4.67	201	4.67
Fortinet	609	4.93	609	4.93	422	6.14	422	6.14	109	18.94	109	18.94	106	8.85	106	8.85
Frisk	386	7.78	386	7.78	327	7.92	327	7.92	103	20.04	103	20.04	57	16.46	57	16.46
F-Secure	803	3.74	1872	1.61	346	7.48	373	6.94	172	12.00	282	7.32	150	6.25	162	5.79
G Data	1087	2.76	1087	2.76	195	13.28	195	13.28	262	7.88	262	7.88	165	5.69	165	5.69
Ikarus	132	22.76	NA	NA	277	9.35	277	9.35	392	5.27	392	5.27	123	7.63	123	7.63
K7	375	8.01	375	8.01	264	9.81	264	9.81	76	27.16	76	27.16	47	19.96	47	19.96
Kaspersky	3120	0.96	3120	0.96	277	9.35	277	9.35	370	5.58	370	5.58	265	3.54	265	3.54
Kingsoft Adv.	17	176.75	2084	1.44	120	21.58	128	20.23	431	4.79	433	4.77	64	14.66	64	14.66
Kingsoft Std	3291	0.91	3291	0.91	197	13.14	197	13.14	775	2.66	775	2.66	69	13.60	69	13.60
McAfee	26	115.57	1451	2.07	268	9.66	297	8.72	282	7.32	279	7.40	186	5.04	173	5.42
Microsoft	1315	2.29	1315	2.29	376	6.89	376	6.89	149	13.85	149	13.85	94	9.98	94	9.98
Quick Heal	1058	2.84	1674	1.79	88	29.42	86	30.11	323	6.39	328	6.29	118	7.95	131	7.16
Sophos	20	150.24	1307	2.30	288	8.99	318	8.14	275	7.51	197	10.48	111	8.45	143	6.56
Symantec	1363	2.20	1368	2.20	171	15.14	178	14.55	228	9.05	228	9.05	109	8.61	109	8.61
Trustport	1807	1.66	1807	1.66	444	5.83	444	5.83	403	5.12	403	5.12	263	3.57	263	3.57
VirusBuster	343	8.76	1302	2.31	230	11.26	235	11.02	156	13.23	213	9.69	84	11.17	109	8.61

is available seems rather improbable – few other products offer the option to only detect *Microsoft Office*-related malware.

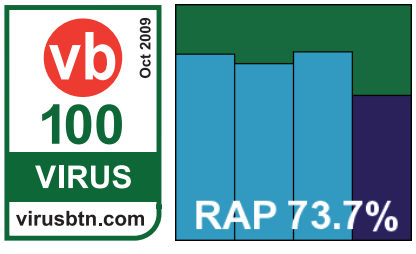
Scanning speeds were impressive and on-access overheads feather-light. A few times during on-demand scans the product tripped up and presented its own error console report, but on-access protection remained stable and restarting the scan proved simple. Detection rates were decent, with some good improvement in the RAP scores, and the clean set was also handled with aplomb.

As expected from the results of other products based on *Frisk*'s technology however, a handful of Virut samples were missed in the WildList set, and *F-PROT* does not win a VB100 award.



F-Secure Anti-Virus for Windows Servers 8.01 build 207

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	91.11%
Worms & bots	100.00%	**False positives**	0



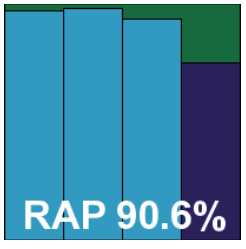
F-Secure's server product bears little evident difference from the standard desktop ranges. The install follows the standard path and needs no reboot, running through fairly speedily. The interface is simple, cool and clear with a good level of configuration, and scanning and protection throughout seemed stable and well-behaved.

For the on-demand scans of the infected sets a command-line tool was used, as logging issues have caused problems in the past, but for all other tests including the speed measurements standard GUI scans were used. These showed the usual rather heavy overheads on access, especially with full-depth scanning enabled (something not recommended by the manufacturer), but on-demand speeds were much more impressive. Detection rates were similarly impressive, scoring fairly well across the board, and with no problems in either the WildList or the clean sets, *F-Secure* thus comfortably earns another VB100 award.

G Data AntiVirus 10.5.51.2

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.25%
Worms & bots	100.00%	**False positives**	0

In the past *G Data* has mainly taken part in our desktop comparatives, missing out on the server tests, but it recently emerged that this was due to some miscommunication and the company does indeed



File access lag time (Time = s; Lag = s/MB)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag	Time	Lag
AhnLab	57	0.02	NA	NA	248	0.09	NA	NA	400	0.16	NA	NA	226	0.21	NA	NA
Alwil	22	0.01	563	0.19	144	0.05	205	0.07	166	0.05	225	0.08	91	0.06	108	0.08
Authentium	53	0.02	177	0.06	383	0.14	392	0.14	351	0.14	389	0.16	177	0.15	231	0.21
AVG	9	0.00	NA	NA	383	0.14	394	0.15	264	0.10	287	0.11	161	0.14	198	0.18
Avira	30	0.01	145	0.05	154	0.05	196	0.07	314	0.12	437	0.18	220	0.20	356	0.34
BitDefender	42	0.01	1031	0.34	223	0.08	256	0.09	371	0.15	399	0.16	205	0.18	215	0.19
CA	38	0.01	NA	NA	147	0.05	147	0.05	170	0.05	170	0.05	84	0.05	84	0.05
eScan	291	0.10	885	0.29	376	0.14	376	0.14	543	0.23	577	0.25	338	0.32	462	0.46
ESET	19	0.01	NA	NA	119	0.04	119	0.04	365	0.15	365	0.15	245	0.23	245	0.23
Filseclab	11	0.00	NA	NA	52	0.01	NA	NA	342	0.14	NA	NA	49	0.02	NA	NA
Fortinet	544	0.18	544	0.18	377	0.14	377	0.14	139	0.04	139	0.04	100	0.07	100	0.07
Frisk	44	0.01	NA	NA	337	0.12	337	0.12	147	0.04	147	0.04	77	0.05	77	0.05
F-Secure	31	0.01	2529	0.84	424	0.16	494	0.18	316	0.12	399	0.16	243	0.22	282	0.26
G Data	240	0.08	240	0.08	515	0.19	515	0.19	737	0.33	737	0.33	305	0.29	305	0.29
Ikarus	134	0.04	NA	NA	289	0.11	289	0.11	225	0.08	225	0.08	129	0.10	129	0.10
K7	48	0.01	NA	NA	250	0.09	250	0.09	148	0.04	148	0.04	91	0.06	91	0.06
Kaspersky	34	0.01	3772	1.25	274	0.10	325	0.12	426	0.18	482	0.20	292	0.28	332	0.32
Kingsoft Adv.	15	0.00	NA	NA	137	0.05	137	0.05	487	0.21	487	0.21	93	0.06	93	0.06
Kingsoft Std	14	0.00	NA	NA	194	0.07	194	0.07	822	0.37	822	0.37	101	0.07	101	0.07
McAfee	20	0.01	1293	0.43	296	0.11	300	0.11	386	0.16	385	0.16	249	0.23	252	0.23
Microsoft	39	0.01	NA	NA	370	0.14	370	0.14	207	0.07	207	0.07	133	0.11	133	0.11
Quick Heal	5	0.00	NA	NA	76	0.02	NA	NA	259	0.10	NA	NA	107	0.08	NA	NA
Sophos	32	0.01	1100	0.36	296	0.11	319	0.12	183	0.06	211	0.07	131	0.10	146	0.12
Symantec	18	0.00	NA	NA	122	0.04	122	0.04	194	0.06	194	0.06	87	0.06	87	0.06
Trustport	88	0.03	3138	1.04	623	0.23	744	0.28	679	0.30	749	0.33	420	0.41	456	0.45
VirusBuster	16	0.00	NA	NA	236	0.08	239	0.09	127	0.03	181	0.06	134	0.11	157	0.13

provide a full range of corporate and server solutions. Due to timing issues our first look at the server offering was provided in German only, but thanks to the remarkable linguistic talents of the lab team it was fairly simple both to set it up and to use it.

The install process involves setting up a management tool and deploying to individual clients (in this case the local machine) from there, but unlike many such tools it performed its task without fuss or obstacle, despite the language issue.

The control centre, based in the management tool, provides a detailed range of controls and monitoring tools, with some nice statistics reporting. The raw logging, required by us to gather detailed detection data, was a little gnarly

Reactive And Proactive (RAP) detection scores	Reactive			Reactive average	Proactive	Overall average
	week -3	week -2	week -1		week +1	
AhnLab V3Net	70.60%	59.20%	49.30%	59.70%	27.00%	51.53%
Alwil avast!	93.20%	94.30%	91.50%	93.00%	55.40%	83.60%
Authentium Command	74.40%	73.40%	63.10%	70.30%	41.20%	63.03%
AVG I.S. Network Edition	92.60%	91.70%	90.00%	91.43%	61.10%	83.85%
Avira AntiVir Server	96.30%	91.80%	89.90%	92.67%	59.00%	84.25%
BitDefender Security	88.00%	86.20%	83.30%	85.83%	65.60%	80.78%
CA eTrust	44.60%	36.20%	34.40%	38.40%	23.10%	34.58%
eScan Internet Security	88.00%	86.30%	83.20%	85.83%	65.40%	80.73%
ESET NOD32	93.40%	94.80%	91.20%	93.13%	70.00%	87.35%
Filseclab Twister	46.80%	39.80%	44.50%	43.70%	29.00%	40.03%
Fortinet FortiClient	60.50%	23.00%	41.50%	41.67%	16.10%	35.28%
Frisk F-PROT	74.60%	73.40%	63.90%	70.63%	41.40%	63.33%
F-Secure Anti-Virus	78.70%	75.00%	79.80%	77.83%	61.30%	73.70%
G Data AntiVirus	96.60%	97.70%	93.20%	95.83%	75.00%	90.63%
Ikarus virus.utilities	97.20%	98.50%	95.90%	97.20%	76.50%	92.03%
K7 Total Security	74.40%	64.30%	59.20%	65.97%	35.60%	58.38%
Kaspersky Anti-Virus	76.10%	67.20%	73.30%	72.20%	52.20%	67.20%
Kingsoft I.S. 2009 Advanced	28.40%	24.30%	31.10%	27.93%	17.50%	25.33%
Kingsoft I.S. 2009 Standard	15.00%	12.30%	21.20%	16.17%	8.00%	14.13%
McAfee VirusScan Enterprise	88.10%	86.50%	83.40%	86.00%	59.90%	79.48%
Microsoft Forefront	93.00%	90.80%	89.40%	91.07%	68.40%	85.40%
Quick Heal AntiVirus Lite	76.10%	60.90%	59.60%	65.53%	30.10%	56.68%
Sophos Anti-Virus	88.70%	83.40%	81.00%	84.37%	58.70%	77.95%
Symantec Endpoint Protection	94.30%	91.30%	50.70%	78.77%	24.40%	65.18%
Trustport Antivirus 2009	98.20%	98.50%	96.80%	97.83%	77.60%	92.78%
VirusBuster for Servers	79.10%	74.90%	70.10%	74.70%	40.80%	66.23%

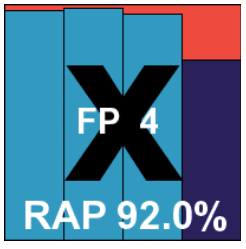
to handle and in places seemed a little malformed, perhaps due in part to the system halting unexpectedly during one of the heavier scan runs (we were delighted to note, however, that scanning continued where it had left off as soon as the system was back online).

In the final reckoning, we found just what we had expected from the multi-engine approach: some fairly slow scanning speeds but quite jaw-dropping detection rates, including an average of over 90% for the four weeks of the RAP test. With barely a thing missed anywhere including in the WildList, and no issues with false positives either, *G Data* easily wins another VB100 award.

Ikarus virus.utilities 1.0.108

ItW	99.87%	**Polymorphic**	73.93%
ItW (o/a)	99.87%	**Trojans**	98.54%
Worms & bots	99.88%	**False positives**	4

Ikarus, having first entered a *VB* comparative many years ago, became a semi-regular entrant in the tests for a while before dropping out of sight again for the past year. Back in again at last, we were intrigued to see what improvements had been made in the intervening months. Initially there was little to see, with the install and interface much as remembered, although the product's stability seemed greatly improved. The design is fairly basic and provides minimal configuration, and is occasionally a little tricky to navigate, but generally works well. On a couple of occasions we noticed the main interface freezing up for periods during on-access testing of large numbers of infected samples, but few real-world users are likely to put their product under such strain, and it soon righted itself once the bombardment was over.

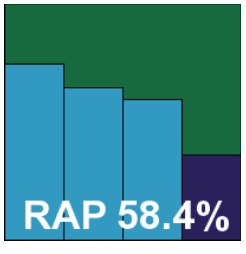


Looking through the results we saw some very good speeds in both measures, and detection results were really quite remarkable, powering effortlessly through the RAP and trojan sets with barely a sample undetected even in the week +1 set. Viruses proved to be less of a specialty however, with slightly lower scores in the polymorphic set and a fair number of Virut samples also not detected. Along with a handful of false positives from items recently added to the clean set, including files from major houses such as *Oracle* and *Sun Microsystems*, *Ikarus* does not quite reach the required standard for a VB100 award this time, and is also denied the chance to see its superb scores recorded on our cumulative RAP quadrant, but judging by the general excellence of detection looks likely to take its first award very soon.

K7 Total Security Desktop Edition 10.0.0015

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.09%
Worms & bots	100.00%	**False positives**	0

K7 has become a fixture in our tests in the past year or so, and has slowly drawn closer to the required mark, with its sporadic failures to achieve certification caused by increasingly minor issues. The now familiar product has an extremely fast and simple install process, and presents a pleasant and colourful interface which proved easy to navigate and use. A few problems did emerge during testing, including a dreaded blue screen during the on-demand scan of the infected sets, but the problem did not recur on retrying the scan. We also had some problems persuading the scheduler to operate.

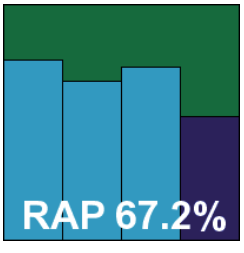


These issues aside, scanning speeds were quite excellent on demand, and on-access overheads were also highly impressive. Detection rates continue to improve in both the trojans and RAP sets, and handling of polymorphic items, including those in the WildList, was faultless. With no further problems with false positives, *K7* continues its VB100 odyssey with another award.

Kaspersky Anti-Virus 6 for Windows Servers Enterprise Edition 6.0.2.555

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.24%
Worms & bots	100.00%	**False positives**	0

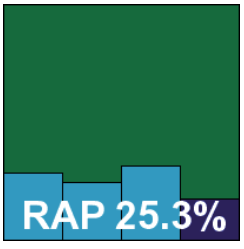
Kaspersky provides another proper server-oriented product, again using the MMC as its control console. The management tool requires separate installation from the main protective component, and it took some time to explore and familiarize ourselves with the rather complex layout, some useful options being rather hard to find; users may be best advised to read the full manual before deployment. We also noted some more frustrating behaviours, including scan options resetting themselves when other areas of configuration are changed.



Despite the awkwardness and misbehaviour of the interface, testing proceeded without major difficulties, and as usual the thoroughness of the protection led to some slowish scan times and fairly heavy overheads. Detection rates were generally pretty good, perhaps not quite as high as expected over the RAP sets, but there were no problems in the WildList or clean sets and *Kaspersky* duly qualifies for a VB100 award.

Kingsoft Internet Security 2009 Advanced Edition 2008.11.6.63

ItW	99.99%	**Polymorphic**	61.94%
ItW (o/a)	99.99%	**Trojans**	21.20%
Worms & bots	99.58%	**False positives**	0

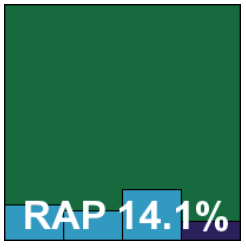


Kingsoft once again provided two products that are indistinguishable on the surface. The install for both is fairly zippy and straightforward, with no major obstacles and no reboot required, although the registering of some services after the initial install process does take a few moments. The interface is rather plain and un-jazzy, but provides a basic set of configuration with some clarity and ease of use. A prompt offers to update the product before any on-demand scan, to ensure maximum detection, which is an interesting touch.

Scanning speeds were pretty good and overheads around average, but detection rates left much to be desired, especially in the RAP and trojans sets. The WildList set, with its large complement of Virut samples, proved too much this time, with several samples of one of the two strains missed, and despite no false positives *Kingsoft* is denied a VB100 award for its Advanced edition.

Kingsoft Internet Security 2009 Standard Edition 2008.11.6.63

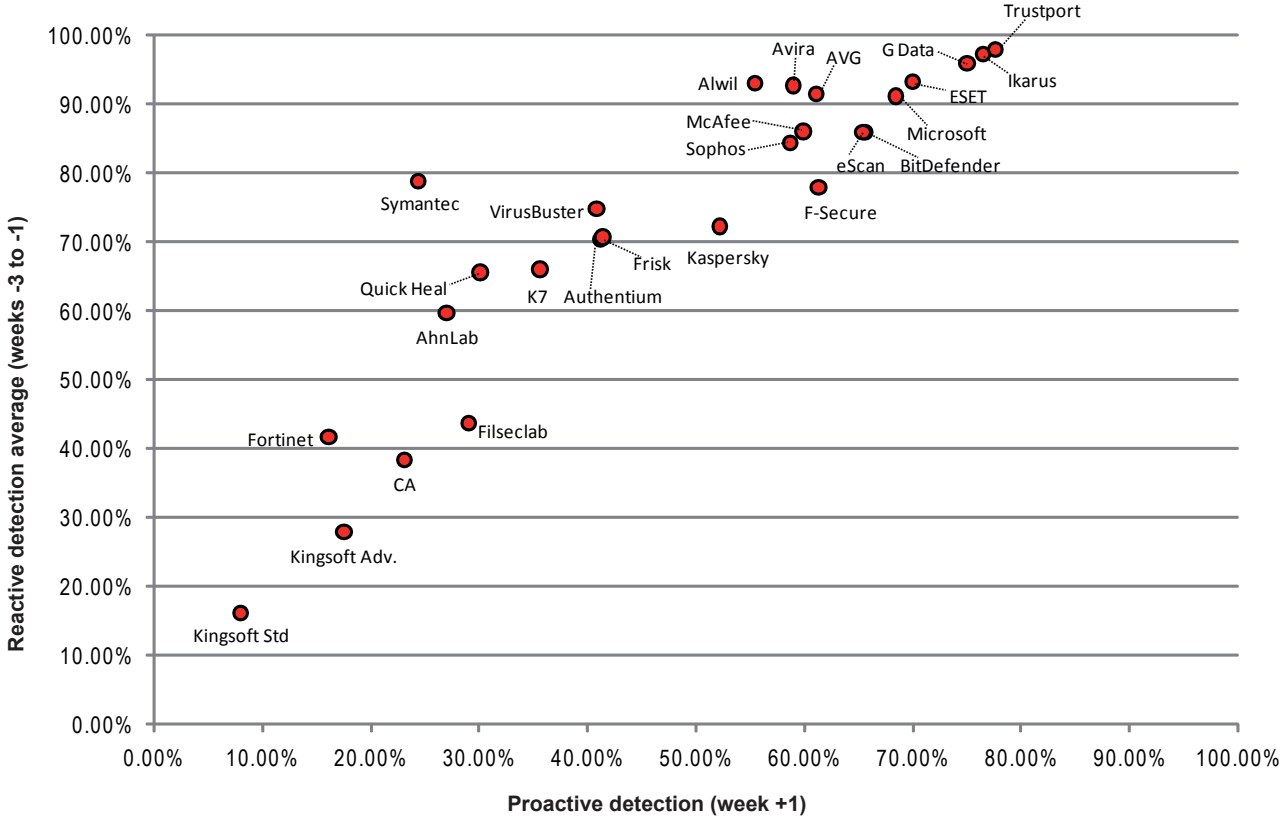
ItW	99.91%	**Polymorphic**	59.94%
ItW (o/a)	99.91%	**Trojans**	7.20%
Worms & bots	99.54%	**False positives**	0



As mentioned above, the Standard version of *Kingsoft*'s product is all but impossible to tell apart from the Advanced one, and provides an identical installation and operation experience, including the option to join a community scheme sharing data on attacks and infections.

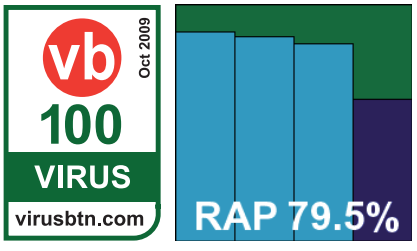
As on previous occasions, however, this version proved less 'advanced' than its counterpart in many ways, including much less impressive performance in the speed tests and even lower scores in the infected sets. Again no false positives were recorded, but fairly large numbers of samples of both Virut strains went undetected, and *Kingsoft*'s second chance at a VB100 is also doomed.

Rap detection scores – October 2009



McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.62%
Worms & bots	100.00%	**False positives**	0

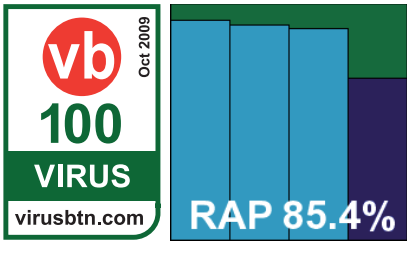


McAfee's corporate product remains its sober and sensible self, barely changed for the past several years. No problem there for us, as it remains as solid, stable and well-behaved as ever. Installation and set-up presented no problems, with a comprehensive range of options available to suit the most demanding administrator. Changing these settings produced one oddity noted here before: on-access protection remains inactive for a few seconds after it has been switched on and is claimed to be operational by the interface – but it seems unlikely that this tiny window will present much of an opportunity for infection.

The product does include one new item added in recent months: the option to use the company's 'in-the-cloud' look-up system to improve protection – but as this is disabled by default in the corporate line it could not be included in VB100 results even were it logistically possible. Even without it, detection rates were pretty decent across the board, although scanning speeds were no more than reasonable, and with no problems handling our polymorphic samples or clean sets *McAfee* easily wins another VB100 award.

Microsoft Forefront Client Security 1.5.1972.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	92.57%
Worms & bots	100.00%	**False positives**	0

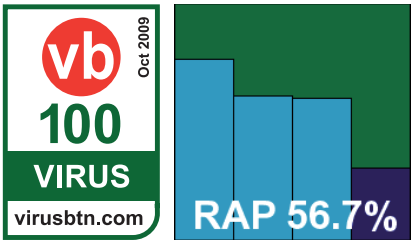


Microsoft's corporate product is another which remains little changed after many tests, and we hope to see it joined in the next comparative by a shiny new sibling in the shape of the free *Security Essentials* product, formerly codenamed 'Morro'. The install process is somewhat complicated by the demands of our lab set-up, and the interface remains almost completely lacking in controls, but with a reasonable set of defaults the product had no problem powering through the tests.

Scanning speeds leaned towards the better end of the scale, and detection rates showed a continuation of *Microsoft*'s inexorable improvement, with some excellent scores in the RAP sets once again. No problems were encountered in the WildList or clean sets, and *Microsoft* takes another VB100 award comfortably in its stride.

Quick Heal AntiVirus Lite 10.00

ItW	100.00%	**Polymorphic**	98.28%
ItW (o/a)	100.00%	**Trojans**	81.41%
Worms & bots	99.88%	**False positives**	0

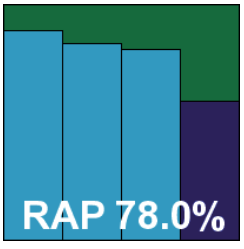


Quick Heal continues to carve its own special furrow with the smallest, fastest and simplest installer and its usual remarkable simplicity and speed. The interface, once up and ready a few moments after starting the installation, is pared down and attractive, but manages to provide a fair range of options under the hood. Some server admins may find the lack of option to scan all file types on access a rather significant omission – but additional file types can be added manually to the extension list.

Setting up scans took a little longer than expected, with a considerable lag after pressing the browse button, but once up and running it produced some decent speeds – perhaps less impressive than usual over some sets, but way ahead of the field over the most significant set of binaries. On access, lag times were pretty superb too. Detection rates were fairly decent, with a notable and somewhat strange drop in detection between on-demand and on-access over the trojans set, which was confirmed by multiple retries. The WildList was handled without issue though, and with no false alarms either, *Quick Heal* adds another VB100 award to its trophy cabinet.

Sophos Anti-Virus 7.6.10

ItW	99.99%	**Polymorphic**	100.00%
ItW (o/a)	99.99%	**Trojans**	90.60%
Worms & bots	100.00%	**False positives**	0

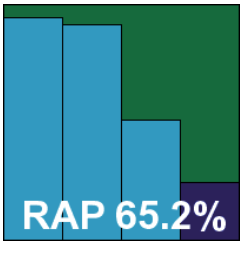


Sophos's product is another that has remained unchanged on the surface since time immemorial, with a pleasantly easy install process remarkable only for the offer to remove third-party security software. Configuration is available in multiple levels going to extreme depth, and is generally simple to use although the setting up of on-demand scans proved slightly more fiddly than necessary. On one occasion, by carefully meddling with the product settings while subjecting it to heavy bombardment with infected samples, we managed to freeze the test machine, but could not repeat this feat.

Performance in the speed tests was very good indeed, and detection rates generally excellent too, with a very shallow decline across the reactive portion of the RAP sets hinting at few issues keeping up with the influx of new items. No false positives were alerted on, but in the WildList set a single sample of one of the W32/Virut strains was not detected. Further investigation found no further such samples even after producing many tens of thousands more, but the developers were able to diagnose the issue and pinned it down to a small window of a few days either side of the submission date, when detection for a tiny percentage of Virut samples was temporarily broken. Despite the rarity of such examples, a single miss is all it takes under our strict rules, and *Sophos* is unlucky to miss out on a VB100 award this month.

Symantec Endpoint Protection 11.0.4014.26

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	92.13%
Worms & bots	100.00%	**False positives**	0



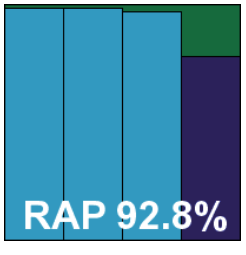
Symantec's corporate product had a facelift not so long ago, giving it a much more colourful, curvy appearance which has not been popular with everyone here. However, a fresh pair of eyes on it this month found that while the install process is perhaps rather more complex than required, with a reboot needed to complete, the interface itself is fairly usable and pleasant to operate. Configuration is fairly thorough although limited in some areas, and the interface takes a few seconds to update its displays when a major configuration change is in place. In many cases this is perhaps a good thing, though, it being better to warn that protection is not yet ready when it is in fact up and running than to prematurely proclaim full operation.

Testing tripped merrily along with some decent on-demand speeds and some excellent on-access overheads, and while on-demand scans of the infected sets were slow in the extreme – taking several days where the fastest products handled the same sets in less than an hour – few real-world users will be running scans anything like as large as ours.

Logging as usual is provided in vast detail, usually far too much for the interface to handle and somewhat fiddly to extract from the raw data, but results were eventually obtained and showed some excellent detection rates over older samples, dropping off rather sharply in the most recent reactive week of the RAP set. No issues with false positives were observed, and in the WildList and polymorphic sets *Symantec* showed it has recovered from the minor stumble of the last comparative and is once again a comfortable winner of a VB100 award.

Trustport Antivirus 2009 5.0.0.4041

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	97.97%
Worms & bots	100.00%	**False positives**	0



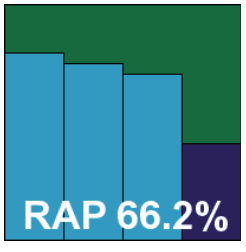
Trustport is another multi-engine product. This first becomes evident during the install when, among the standard set-up choices, an option is provided to perform some advanced configuration of the engines and the way in which they are used. These same choices can also be made at any time from within the main configuration interface. The control system is somewhat unusual, providing a selection of separate mini-GUIs for different purposes, but the central control panel provides most requirements in ample depth.

As expected, the multi-engine approach does not make for the best speeds, and on-access overheads are also pretty heavy, but detection rates were stratospheric, pushing perfection in most areas and highest of all this month's entrants in all the RAP weeks. With this excellence carried over to the standard sets and not balanced, as might be

expected, by any false alarms, *Trustport* is more than worthy of a VB100 award.

VirusBuster for Servers 6.1.163

ItW	99.99%	**Polymorphic**	90.43%
ItW (o/a)	99.99%	**Trojans**	79.92%
Worms & bots	99.92%	**False positives**	0



Another proper server product with another MMC interface to provide the controls, *VirusBuster*'s server offering has a fairly standard installation but proves a little less straightforward to operate once up and running. The layout within the GUI is complex and at times a little confusing. In some parts it lacks uniformity with other areas, and it is easy to confuse the GUI by clicking too impatiently on slow-to-respond buttons. Nevertheless, with some patience a decent level of control is available, although the option to scan archives on access, which seems clear, appears to have no function.

With everything set up according to our requirements, testing progressed apace thanks to some highly impressive scanning speeds in both modes, and produced some very commendable detection figures. Most test sets were handled well, but for the last time this month one of those sets of Virut samples proved too much to handle, and *VirusBuster* misses out on a VB100 award despite an otherwise generally decent performance.

CONCLUSIONS

Another month, another comparative, another set of highs and lows. On the plus side, this month we saw very few false positives – perhaps mostly thanks to a relatively small update to the clean sets. We also observed much less instability this month than in the last comparative, with only a handful of crashes and freezes, most of which proved to be one-offs. Of course, it could be that this was helped along by the stability of the platform, which proved remarkably resilient at all times.

We saw a good selection of products, both regular desktop editions and dedicated server products, with some interesting additional features likely to be of interest to the server administrator.

The results of our RAP tests continue to develop trends and patterns, with most products scoring consistently in line with previous performances, and a new arrival looking set to make some considerable waves on our cumulative quadrants once false positive issues are eliminated. The most interesting part of the RAP results is not the pure numbers but their interrelation week on week, with steep downward curves hinting at some lag between the appearance of samples and inclusion of detection. The proactive week also indicates good response times, with some detections being added even before *VB* has had first sight of a sample, as well as heuristic and generic detection of truly unknown items.

The dominant issue this month has, of course, been the pair of highly complex polymorphic file-infecting viruses in the WildList. The large sample sets we were able to include, thanks to an automated generation and validation system, have cut a swathe through the field of entrants once again, separating those whose coverage is flawless (or nearly so) from those that have some improvements to make. A couple of products were hit by single, highly rare and unusual samples which tested their detection to breaking point, and while some may feel hard done by, we feel it is required of us to ensure that we test detection of the WildList as thoroughly and completely as possible. We may need to impose some limits however, if only for the sake of our own sanity and the time restrictions of the test, and plan to include some detail on our policy on virus replication in an update to our general procedures, expected soon. We will also continue to monitor how other areas of the procedures are performing.

In the next comparative review (due for publication in the December issue of *VB*), we should see a major and exciting new platform for the VB100, with the next test deadline expected just a few days after the official public release date of *Microsoft*'s new *Windows 7*. Assuming all goes well with the release, we expect to see a record number of products joining the comparative, and hope to make a few further improvements to our tests. As always, we welcome suggestions on any further information which may be of value or interest to our readers.

Technical details

Test environment: All products were tested on identical systems with *AMD Athlon64 X2* Dual Core 5200+ processors, 2 GB RAM, dual 80GB and 400GB hard drives, running *Microsoft Windows Server 2008 Standard Edition, Service Pack 2, 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.