COMPARATIVE REVIEW

VB100 ON WINDOWS 2003 SERVER X64

John Hawes

This month's comparative review tackles the 64-bit version of *Windows Server 2003*. Although superseded by *Server 2008* last year, the platform remains the standard server OS in many *Windows* environments, and as such it should be well provided for by anti-malware solutions.

The platform presents a number of issues for developers to overcome, not least the 64-bit environment, whose unexpected quirks and oddities seemed certain to show up in the performance of a few products – especially those not specifically built for the environment. Several potential pitfalls presented by the WOW64 system were highlighted at a recent conference on vulnerabilities, where researchers documented the possibility for numerous products to be deceived by the doctored responses returned by the set-up. Many other issues, particularly with built-in emulation, also seemed likely to crop up.

A slightly larger than anticipated field of competitors entered the fray this month, despite a couple of unexpected absentees. A total of 22 products made the final list, many of them dedicated server products but with a fair share of standard desktop editions as well. A single newcomer bravely took its first stand against the VB100 system on this tough platform, with most of the other entrants familiar through long histories in our tests.

PLATFORM AND TEST SETS

Initial set-up and configuration of the operating system is not too complex or demanding a task, particularly as our requirements were for little more than a basic fileserver system – the main aim of our test is to measure the abilities of the products to protect both the local system and other systems accessing files stored on it, and the more complex side of server administration – running web, mail and database servers and so on – was outside of our remit. Beyond installing the OS, overlaying the latest service pack and applying some network drivers required to activate the network cards, little additional manipulation was required to get the systems set up to our liking.

With snapshots of the test systems taken, test sets were copied to shares on each machine. This month's test set deadline was 17 April – rather earlier than usual to accommodate the new RAP set-up and a slew of important conferences taking place around the start of May, and this unfortunately meant missing the release of an updated WildList by a matter of days. As usual, we went with the

most up-to-date list available at the time of the deadline: the February 2009 list, released in late March. This meant that there would have been plenty of time for labs to ensure full coverage, and it also meant that only fairly minor changes to our core certification set needed to be made. Additions consisted mainly of the standard autorun worms and online gaming trojans which have been dominating the list for some time, with a sprinkling of new W32/Conficker variants as the main item of interest. One of the most highly anticipated additions, a new strain of the complex W32/Virut polymorphic file infector, did not quite make it onto this list – making its debut in the March list (so likely to appear in our WildList set in the next VB100 review) – but as samples were rife in our feeds in the month prior to the test we were able to include a large batch in our polymorphic set.

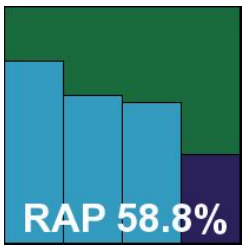
The size of this batch was considerably enhanced by an automated virus replication tool which has been under development in the lab for some time. After having reached a reliable state, the tool has been churning out large numbers of new samples throughout the last few months. This has enabled us to refresh and enlarge several of our polymorphic test sets, with several of the more virulent W32/Virut strains now represented by several thousand samples. With the latest strain well represented here, we were promised some insight into how well labs have dealt with this tricky, highly prevalent and now officially in-the-wild threat.

Elsewhere, the RAP and trojan test sets were made up of recent items arriving from our various sample sources, with the RAP samples gathered in the three weeks prior to the product deadline and the week after it, and the trojan set built from items appearing in the month or so prior to that. We had hoped to find time to rebuild and refresh our set of worms and bots, and did put together a semi-validated set for this purpose, but regrettably we were unable to perform the necessary steps to complete the integration; the VB100 review on *Vista* (due for publication in August) should see this set stocked with fresh items from the same period as the trojans set.

The clean set saw a fairly standard-sized update, with the bulk of new additions consisting of drivers and firmware for network devices and tools. With everything ready, all systems matching and sets synchronized, we got down to finding out how the products would fare.

Agnitum Outpost Security Suite Pro 2009 6.5.4.2525.381.0687

ItW	100.00%	**Polymorphic**	88.58%
ItW (o/a)	100.00%	**Trojans**	80.78%
Worms & bots	99.91%	**False positives**	0



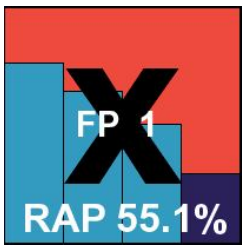
Agnitum's *Outpost* suite is essentially a desktop product, but should provide ample protection for a server platform. The installation process includes options for the numerous components, including web and spam filtering and behavioural monitoring as well as the famed client firewall. Installation took quite some time thanks to various network scans, attempts to update (foiled of course by the isolated nature of our lab), and finished with a recommendation to reboot to ensure full efficacy.

Once ready to use, the interface impressed the lab team with its simple, uncluttered layout, but it seemed somewhat lacking in the fine-tuning options likely to be required by most server admins to ensure best fit with their specific requirements. Scanning speeds were no more than fairly good, and on-access lags were somewhat above average, but a caching system should provide better speeds once the product has familiarized itself fully with its environment (something which we hope to be able to test more accurately in the near future). Our tests didn't cover the behavioural and other aspects of protection provided, but the detection rates recorded represent a fair measure of the product's ability to protect fileshares from infiltration. These rates proved fairly decent in general, with a steady decline in detection of the RAP sets as time to product freezing drew closer, as expected. In the polymorphic set, a fair number of samples of the latest Virut variant were missed, suggesting that some more work may be needed to make the grade next time around, but with no issues in the current WildList set, no false positives and no other problems, *Agnitum* starts this month's comparative off well by winning a VB100 award.

AhnLab V3NET for Windows Servers 7.0.2.2

ItW	100.00%	**Polymorphic**	98.92%
ItW (o/a)	100.00%	**Trojans**	75.38%
Worms & bots	99.86%	**False positives**	1

AhnLab's dedicated server product proved much simpler to install, with the option of a pre-install scan to ensure the system is clean before getting under way. The install offers an optional 'anti-hacking' feature alongside the standard choices, and is up and running with no reboot required. The interface,



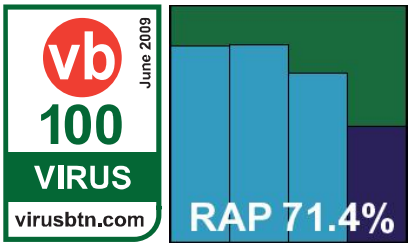
closely mirroring the desktop product, is clean and simple with most of the basics easy to find, but once again, the more in-depth configuration which seems appropriate for server products was absent.

Speeds were somewhat slow on demand, but not bad at all on access. Detection rates also seemed fairly impressive, with again a pretty steady decline across the RAP sets as expected, and mediocre coverage of the latest Virut variant.

In the WildList set, things seemed fine on demand but less so on access, where a small selection of samples were not blocked immediately. Probing this issue, it seemed that the product continues the somewhat outmoded path of separating 'virus' and 'spyware' detection, to the extent of requiring separate filesystem scans to check for each type of malware. Both types of detection are active on access, and some WildList samples were being detected by the anti-spyware portion of the product. Despite appearing to be configured to deny access on detection, the anti-spyware module seemed not to do this as well as the anti-virus module, which was blocked from scanning the files as they had already been alerted on by the anti-spyware component. Although this seems like a rather nasty situation, logging of detection is all that the VB100 rules demand and thus the product is credited with full coverage of the WildList. In the clean sets, a false positive emerged on a fairly obscure browser product, relieving us of the pressure of making a tricky call on the WildList behaviour, and *AhnLab* does not quite make the grade for a VB100 award.

Alwil avast! Server Edition 4.8.1087

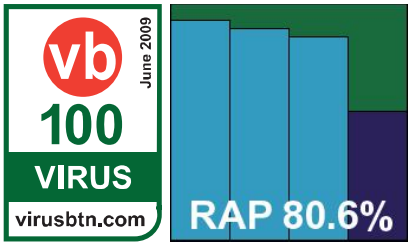
ItW	100.00%	**Polymorphic**	99.22%
ItW (o/a)	100.00%	**Trojans**	94.20%
Worms & bots	99.91%	**False positives**	0



Alwil's server version provides a speedy and straightforward installation process, at the end of which a reboot is not forced, but those choosing not to do so are warned that 'system failure' may result. The interface closely resembles the desktop edition, with the advanced version providing a wide range of controls and options but proving rather cluttered and difficult to navigate. While a simple version is also available, the default settings provided are fairly basic and likely to be inadequate for most admins. Scanning speeds were fairly mid-range, and detection rates a fraction below the outstanding levels expected – but were nevertheless impressive, with no problems having been encountered in detecting the large numbers of new W32/Virut samples in the polymorphic set. The WildList was likewise covered cleanly, and with the clean set presenting no serious problems either, a VB100 is awarded to *Alwil*.

AVG Internet Security Network Edition 8.5.322

ItW	100.00%	**Polymorphic**	98.96%
ItW (o/a)	100.00%	**Trojans**	96.15%
Worms & bots	99.95%	**False positives**	0



AVG's product again provides a slick and fast install, with no reboot necessary, and a 'first run wizard' provides configuration for things like updating, scheduled scans, trusted networks and so on. The interface seems identical to the standard desktop version – rather busy, with icons for numerous components and modules leading to more advanced configuration in tree format, which can also become a little tricky to navigate in its rather small default window. Some options that would be of relevance to server admins, such as processing of archive files on access, seemed to be absent, but could merely have been overlooked in the confusion.

Speeds were in the medium range, and detection rates continued their recent upward climb, with once again no problems with either the WildList or the new Virut strain expected to join it next time around. The clean sets were ably handled too, and *AVG*'s superb performance earns a VB100 award.

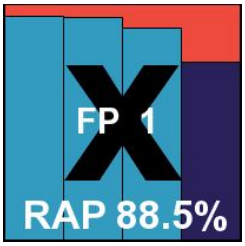
Avira AntiVir Server 9.00.00.23

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.98%
Worms & bots	100.00%	**False positives**	1

Avira also impressed with the speed of its installation process, despite the need to set up some Visual C++ components on the system, and again no reboot was required. This is a proper server edition, with an MMC-based console to control configuration – which appeared to be provided in considerable depth. The neatly laid out tree structure proved simple to navigate and easy to use, and overall the design was declared excellent by the lab

On-access tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	2	99.91%	442	88.58%	1931	77.34%	0	0
AhnLab V3Net	0	100.00%	3	99.86%	246	98.92%	2251	72.47%	1	0
Alwil avast!	0	100.00%	2	99.91%	13	99.22%	538	93.92%	0	0
AVG Internet Security	0	100.00%	1	99.95%	21	98.96%	394	94.56%	0	0
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	241	96.86%	1	1
BitDefender Security	0	100.00%	0	100.00%	0	100.00%	911	87.62%	1	0
CA eTrust	0	100.00%	0	100.00%	1049	92.03%	6743	32.03%	0	0
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	1405	86.70%	0	0
Fortinet FortiClient	0	100.00%	0	100.00%	202	99.15%	8872	5.66%	0	0
Frisk F-PROT	0	100.00%	0	100.00%	165	98.93%	2420	67.74%	1	0
F-Secure Anti-Virus	0	100.00%	0	100.00%	1	100.00%	3184	75.76%	0	2
K7 Total Security	0	100.00%	134	93.72%	760	86.09%	4265	61.82%	0	0
Kaspersky Anti-Virus	0	100.00%	0	100.00%	1	100.00%	3226	74.65%	0	0
McAfee VirusScan	0	100.00%	0	100.00%	1	100.00%	903	87.95%	0	0
MWTI eScan	0	100.00%	6	99.72%	0	100.00%	837	88.71%	0	0
Netgate Spy Emergency	143	69.96%	484	77.33%	9963	1.77%	8163	14.61%	13	0
Norman Virus Control	0	100.00%	0	100.00%	726	81.34%	2677	70.95%	0	0
Quick Heal Anti-Virus	0	100.00%	8	99.63%	178	95.69%	2738	68.28%	1	0
Sophos Anti-Virus	0	100.00%	0	100.00%	4	99.97%	857	88.88%	0	6
Symantec Endpoint Protection	0	100.00%	0	100.00%	1	100.00%	478	93.59%	0	0
TrustPort Antivirus	0	100.00%	0	100.00%	131	98.82%	1441	88.19%	0	0
VirusBuster Professional	0	100.00%	2	99.91%	442	88.58%	2044	78.29%	0	0

team, although the default settings on access were once again fairly basic. Running through the test quickly and easily, we noted that on-demand speeds, normally extremely fast, were not as far ahead of the pack as usual, although on-access overheads were as excellent as ever.



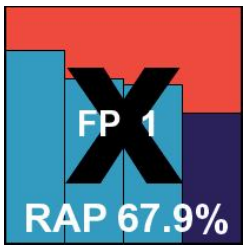
Detection rates were similarly superb across the board, with some truly remarkable figures in the RAP sets and no problems handling the expanded polymorphic sets. Sadly, however, a single false alert on a fairly minor item in the clean sets scuppered *Avira*'s hopes of earning a VB100 this month.

BitDefender Security for Windows File Servers 3.1.70

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	88.36%
Worms & bots	100.00%	**False positives**	1

Another full server edition, *BitDefender* offers admins control over the number of scanning processes implemented, and during installation does some probing to estimate an optimal default level. Also included with the otherwise fairly standard install process is a request for permission to send crash information back to the developers to smooth out any wrinkles in the product's stability, and at the end a reboot is required to finalize the

install. The interface again uses the MMC system and a tree of configuration and option controls, which the team found clear and well laid out. It also provides lots of statistical information on its own performance, which many server admins may find useful, and provides a wealth of other server-oriented extras such as importing schedule settings from a file.



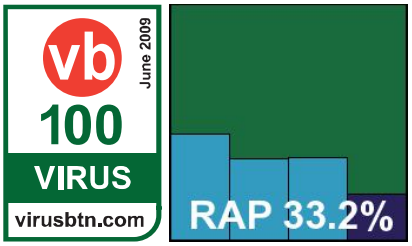
An initial run over the test sets found no problems on access, but the on-demand tests were held up while we tried to persuade the scanner to run. A batch of scheduled scans were set up to run over a weekend but failed to activate, and attempts to kick-start the same jobs manually also proved fruitless. Little information seemed available and it was not even clear whether scans were in fact running in the background and simply snagged somewhere, or not running at all. Reinstalling the product on a fresh system fixed all this however, with no repeat of the odd issues, and all tests were completed without further upset.

Scanning speeds were not excellent, with some rather heavy overheads on access, but detection was very good across all sets, with a gentle decline through the RAP sets but little missed elsewhere, including full coverage of the WildList and polymorphic sets. In the clean test sets, logs confused us for a while with their tendency to include password-protected files in the 'virus' category, and a single item, a component of the popular open-source graphics tool the *Gimp*, was mislabelled as a trojan. *BitDefender* thus also misses out on a VB100 award despite a strong showing.

CA eTrust Anti-Virus 8.1.637.0

ItW	100.00%	**Polymorphic**	92.03%
ItW (o/a)	100.00%	**Trojans**	32.03%
Worms & bots	100.00%	**False positives**	0

CA's *eTrust* is a corporate-focused product and has remained unchanged for several years, although the anti-malware side of the giant company has gone through a major evolution lately and we hope to see a significant overhaul of the product in the near future. Installation was somewhat arduous, with a number of lengthy EULAs which had to be scrolled through to the end to simulate reading them, and a form requiring plenty of personal information. A reboot is required to finalize the process. The interface has never been the most popular with the lab team, but worked better than usual on a server platform, presenting fewer of the slowdowns noted on some desktop tests. Testing ran through at a rapid rate, aided by the product's remarkable scanning speeds. On-access overheads were similarly feather-light, but completing the testing process was somewhat hampered by the product's horribly unfriendly logging format, which required some fairly crude hacking into shape before any useful data could be extracted.

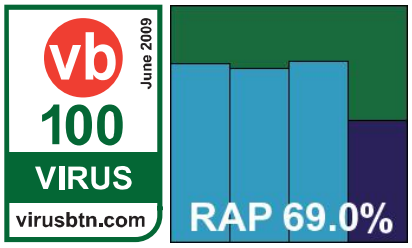


Results were much along the lines of recent experience: fairly mediocre in the trojans and RAP test sets and with some work to do in the polymorphic set too – a fair number of samples of the new strain of W32/Virut were missed. In the WildList set there were no problems however, and with no false positives either *CA* earns another VB100 award.

ESET NOD32 Antivirus Business Edition 4.0.424.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	82.89%
Worms & bots	100.00%	**False positives**	0

ESET's *NOD32* has an excellent history in VB100 testing, with excellence in both detection rates and speeds, but in recent years has lost some ground in the speed area. We were interested to see if the release of version 4 would have any impact on this trend, and initial impressions during installation were fairly promising. There was a brief lag during the 'preparing to install' stage, but otherwise it was a very fast and highly user-friendly set-up process, not needing a reboot to get full protection up and running.



Running through the speed tests first, on-demand settings were pretty thorough by default and throughput seemed fairly sluggish, although it is perhaps unfair to judge against sky-high expectations and in fact it proved to be among the faster products under test, while on-access overheads were barely noticeable. A detailed and well-designed interface appeared well stocked, but a notable omission was the ability to scan archives by default – an option some admins may find useful and one which would have enabled the full running of our speed comparisons.

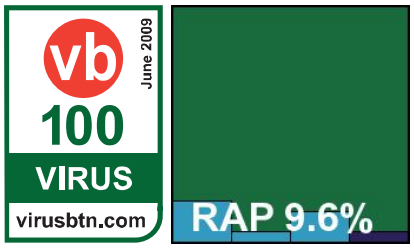
On-demand tests	WildList viruses		Worms & bots		Polymorphic viruses		Trojans		Clean sets		RAP
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.	
Agnitum Outpost	0	100.00%	2	99.91%	442	88.58%	1685	80.78%	0	0	58.8%
AhnLab V3Net	0	100.00%	3	99.86%	246	98.92%	1945	75.38%	1	0	55.1%
Alwil avast!	0	100.00%	2	99.91%	13	99.22%	520	94.20%	0	0	71.4%
AVG Internet Security	0	100.00%	1	99.95%	21	98.96%	290	96.15%	0	0	80.6%
Avira AntiVir	0	100.00%	0	100.00%	0	100.00%	231	96.98%	1	1	88.5%
BitDefender Security	0	100.00%	0	100.00%	0	100.00%	861	88.36%	1	0	67.9%
CA eTrust	0	100.00%	0	100.00%	1049	92.03%	6743	32.03%	0	0	33.2%
ESET NOD32	0	100.00%	0	100.00%	0	100.00%	3384	82.89%	0	0	69.0%
Fortinet FortiClient	0	100.00%	0	100.00%	202	99.15%	8823	6.46%	0	0	9.6%
Frisk F-PROT	0	100.00%	0	100.00%	165	98.93%	2370	68.49%	1	0	48.0%
F-Secure Anti-Virus	0	100.00%	0	100.00%	1	100.00%	3182	75.82%	0	2	69.8%
K7 Total Security	0	100.00%	1	99.95%	1535	75.93%	4111	64.24%	0	0	43.2%
Kaspersky Anti-Virus	0	100.00%	0	100.00%	1	100.00%	2985	78.66%	0	0	69.3%
McAfee VirusScan	0	100.00%	0	100.00%	1	100.00%	893	88.05%	0	0	66.1%
MWTI eScan	0	100.00%	0	100.00%	0	100.00%	839	88.67%	0	0	68.5%
Netgate Spy Emergency	143	69.96%	484	77.33%	9963	1.77%	8166	14.56%	13	0	10.7%
Norman Virus Control	0	100.00%	0	100.00%	507	83.19%	2604	71.99%	0	0	48.4%
Quick Heal Anti-Virus	0	100.00%	5	99.77%	178	95.69%	899	87.95%	1	0	61.9%
Sophos Anti-Virus	0	100.00%	0	100.00%	4	99.97%	857	88.90%	0	6	81.8%
Symantec Endpoint Protection	0	100.00%	0	100.00%	1	100.00%	478	93.59%	0	0	76.0%
TrustPort Antivirus	0	100.00%	0	100.00%	131	98.82%	1705	83.63%	0	0	80.7%
VirusBuster Professional	0	100.00%	2	99.91%	442	88.58%	1734	80.25%	0	0	57.0%

Moving on to the infected sets, things went a little less smoothly. Some quirks in the operation of the on-access scanner meant having to run parts of the test by copying the sets to the test system across the network to activate detection, but this seemed reasonable in a test of fileshare protection. There were also a few occasions when the product seemed overwhelmed by the high stress it was put under, with the interface freezing up for long periods and on one occasion a reboot being needed to get things moving along.

Detection rates in the expanded polymorphic sets were impeccable, and fairly reasonable in the trojan and RAP sets, although perhaps a fraction below the excellent standards we have come to expect. This was thanks in part to a quirk which seemed to cause the on-demand scanner to ignore a fairly large number of items alerted on on-access – as these broadly fell into several clusters of near-identical files, counted as single items when calculating percentages, this impacted more heavily on the raw numbers than the percentage scores, but does seem somewhat worrying. With the WildList covered with no difficulties, however, and no false positives or other issues, *ESET* earns a VB100.

Fortinet FortiClient 4.0.1.54

ItW	100.00%	**Polymorphic**	99.15%
ItW (o/a)	100.00%	**Trojans**	6.46%
Worms & bots	100.00%	**False positives**	0



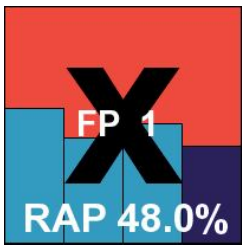
Fortinet's installation process was interrupted by several rather worrying alerts from *Windows* warning that some components were not approved by *Microsoft* and may threaten the stability of the system. Ignoring strong recommendations to abort the install, it continued fairly smoothly, but spent several minutes apparently 'optimizing performance' before the set-up process was complete. Once up and running, a revamped interface presented a smooth and colourful outlook, much more cheery than the previous effort which, while thorough and businesslike, lacked a little charm. It also seems somewhat less cluttered than the old version, while still providing a very good level of configuration and range of fine-tuning options. The defaults, set to thorough and secure, provided a stark contrast with many of the other products looked at so far, which seemed to err on the lax rather than cautious side.

With this thoroughness in evidence in some rather slow scanning speeds, one area where the defaults seemed bizarrely lacking was in the detection capabilities. The standard settings, while capable of handling the WildList quite happily and scoring reasonably well in the other older sets, showed fairly limited coverage of the new Virut strain and miserably low scores across the trojans and RAP sets. Having diagnosed this issue in previous tests, we re-ran scans after activating some additional options. With 'extended databases' enabled, as well as greyware detection and heuristics, detection rates shot up to impressive levels, with a huge leap to over 80% in the trojans set and similar levels achieved across the RAP sets, dropping fairly sharply in the 'Week+1' set.

Admins would be best advised to enable full detection capabilities, but under the VB100 rules defaults must be used (however bizarre they may seem), and the figures reported in our tables thus do not include the additional detections. Activation of the full range seemed to have little impact on the clean sets, with a few additional files labelled as suspicious, and with the default settings not raising any issues at all here a VB100 is duly awarded.

Frisk F-PROT Antivirus 6.0.9.1

ItW	100.00%	**Polymorphic**	98.93%
ItW (o/a)	100.00%	**Trojans**	68.49%
Worms & bots	100.00%	**False positives**	1

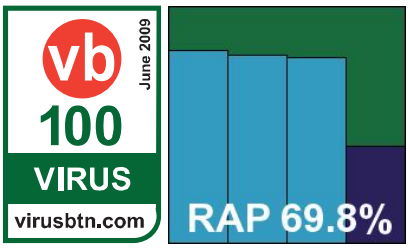


Frisk's *F-PROT* product is a pretty pared-down, bare-bones kind of affair, providing straightforward malware protection for the filesystem, with a little extra in the form of web and mail scanning. The installation process is therefore fairly simple, but seemed a little sluggish at times and needed a reboot to complete. With only basic configuration available, we relied on the defaults to see us through and got the test battery over with fairly quickly, with very good scanning speeds and minimal overheads on access.

Detection rates were a little below expectations in the RAP sets, but much better in the slightly older trojans set and splendid elsewhere, handling all the new Virut samples with aplomb. The WildList proved no problem, but in the clean set a handful of files included with some UPS management software from a major vendor were alerted on by heuristics, which was enough to count as a false alarm under our rules, thus disqualifying *Frisk* from a VB100 award this month.

F-Secure Anti-Virus for Windows Servers 8.00.14130

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	75.82%
Worms & bots	100.00%	**False positives**	0



F-Secure's server edition seems fairly similar to its standard desktop range, although the normal installation process also includes options for centralized or local management policies. Configuration in the simple, sensible interface is available in great depth, although the scheduler seemed to lack sophistication, allowing only a single job with a single target to be specified.

Scanning speeds were, as usual, on the slow side, and on-access overheads pretty hefty, but detection was generally solid, if not quite up to the expected high standards in the RAP and trojan sets. In the polymorphic set, a single instance of the latest Virut variant was not detected, but the WildList set was handled thoroughly. In the clean set, a couple of suspicious alerts were no barrier to *F-Secure* achieving a VB100 award this month.

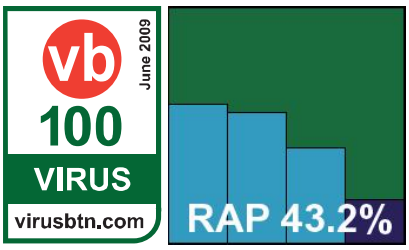
On-demand throughput (MB/s)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)	Time (s)	Thr. put (MB/s)
Agnitum Outpost	954	3.15	954	3.15	217	11.93	217	11.93	127	16.25	127	16.25	90	10.42	90	10.42
AhnLab V3Net	588	5.12	588	5.12	1303	1.99	1303	1.99	170	12.14	170	12.14	903	1.04	903	1.04
Alwil avast!	34	88.50	473	6.36	216	11.99	225	11.51	85	24.28	123	16.78	85	11.04	105	8.93
AVG Internet Security	1806	1.67	1806	1.67	278	9.31	278	9.31	161	12.82	196	10.53	35	26.80	148	6.34
Avira AntiVir	422	7.13	422	7.13	180	14.39	180	14.39	122	16.92	122	16.92	104	9.02	104	9.02
BitDefender Security	1350	2.23	1350	2.23	341	7.59	341	7.59	95	21.73	95	21.73	96	9.77	96	9.77
CA eTrust	262	11.48	262	11.48	50	51.79	50	51.79	43	48.00	43	48.00	30	31.27	30	31.27
ESET NOD32	1363	2.21	1363	2.21	376	6.89	376	6.89	55	37.53	55	37.53	55	17.06	55	17.06
Fortinet FortiClient	304	9.90	304	9.90	345	7.51	345	7.51	56	36.86	56	36.86	68	13.80	68	13.80
Frisk F-PROT	295	10.20	295	10.20	350	7.40	350	7.40	47	43.91	47	43.91	40	23.45	40	23.45
F-Secure Anti-Virus	1504	2.00	1999	1.51	425	6.09	421	6.15	94	21.96	198	10.42	64	14.66	231	4.06
K7 Total Security	136	22.13	NA	NA	213	12.16	213	12.16	31	66.58	31	66.58	34	27.59	34	27.59
Kaspersky Anti-Virus	1850	1.63	1850	1.63	363	7.13	363	7.13	189	10.92	189	10.92	203	4.62	203	4.62
McAfee VirusScan	61	49.33	689	4.37	1070	2.42	1445	1.79	100	20.64	99	20.85	112	8.38	119	7.88
MWTI eScan	521	5.78	521	5.78	1402	1.85	1402	1.85	1142	1.81	1142	1.81	873	1.07	873	1.07
Netgate Spy Emergency	31	97.07	NA	NA	105	24.66	105	24.66	99	20.85	99	20.85	67	14.00	67	14.00
Norman Virus Control	599	5.02	599	5.02	1615	1.60	1615	1.60	58	35.59	58	35.59	136	6.90	136	6.90
Quick Heal Anti-Virus	207	14.54	422	7.13	76	34.07	75	34.52	80	25.80	90	22.93	52	18.04	66	14.21
Sophos Anti-Virus	54	55.72	1636	1.84	399	6.49	523	4.95	69	29.91	165	12.51	35	26.80	213	4.40
Symantec Endpoint Protection	470	6.40	NA	NA	293	8.84	293	8.84	208	9.92	208	9.92	185	5.07	185	5.07
TrustPort Antivirus	925	3.25	925	3.25	339	7.64	339	7.64	118	17.49	118	17.49	120	7.82	120	7.82
VirusBuster Professional	365	8.24	641	4.69	169	15.32	170	15.23	66	31.27	114	18.10	21	44.67	58	16.17

K7 Total Security 9.7.0173

ItW	100.00%	**Polymorphic**	75.93%
ItW (o/a)	100.00%	**Trojans**	64.24%
Worms & bots	99.95%	**False positives**	0

K7's main market is in Japan, but the English version of the product seems pretty smooth and solid. The installation process had a slightly boxy feel, but ran through quickly, with a pause to gather some user information and a reboot at the end. It seemed to make startup slightly slower than expected, but once up and running provided a straightforward and responsive interface with a reasonable level of configuration available. Something that may prove problematic for server admins is the apparent inability to scan more than one level deep into archives, even in thorough on-demand scans.

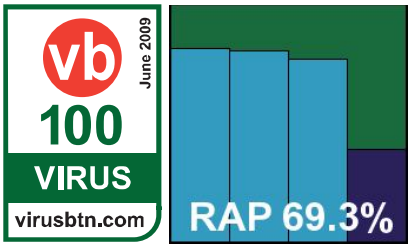
Perhaps thanks in part to these fairly minimal settings, scanning speeds were through the roof, and on-access overheads very low indeed, but detection rates



were medium at best, with a fairly steep week-on-week decline in the RAP sets and large swathes of the new Virut samples not covered. The WildList was handled without any difficulty, and the clean sets likewise, so *K7* also meets the requirements for a VB100 award.

Kaspersky Anti-Virus 6.0 for Windows Servers Enterprise Edition 6.0.2.555

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	78.66%
Worms & bots	100.00%	**False positives**	0

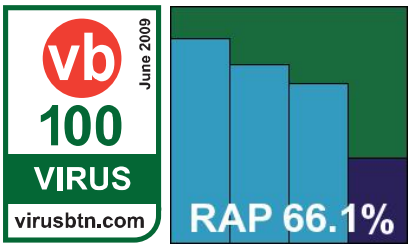


Kaspersky's server edition is a quite separate beast from the company's desktop range, with a long and complex installation process tripping through a large number of options screens. Once the process is complete many admins will also require the administration component, which rather than being an option to the main installer is in fact its own standalone module with a separate set-up process. Once everything is ready, an MMC interface provides a long and complex tree of configuration, monitoring and reporting options. This proved generally fairly simple to navigate, although there were a few moments of confusion thanks to unexpected behaviours and surprising placement of controls. A few times setting changes were rejected, and for a time some error messages appeared to say that the product had lost connection to itself. Most disturbingly, the on-demand scan settings seemed to constantly revert to defaults when changing views from one tab to another, leading to several frustrating runs through the tests as samples were trashed against our instructions. This could be a fairly serious issue in enterprise environments, where experienced admins will want to know exactly what has been found on their networks – with physical copies of files so they can be analysed and any potential breach of data privacy recorded.

Finally gathering the required data for the infected sets, detection rates proved good, but not as excellent as usual, with a sharp drop in the 'Week+1' RAP set contrasting sharply with the desktop product's performance in the last comparative (see *VB*, April 2009, p.15). Nevertheless, scores were still commendable, the WildList was covered without difficulty, and with no false positives, a VB100 award is duly granted.

McAfee VirusScan Enterprise 8.7.0i

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	88.05%
Worms & bots	100.00%	**False positives**	0

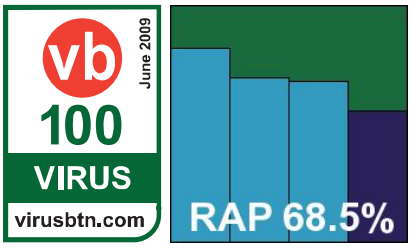


While most competitors have evolved their installers and interfaces into more shiny, colourful and cuddly versions, *McAfee*'s set-up remains sober, sensible and grey. The GUI is simplicity itself, but all the options an admin could desire are neatly tucked away in its easy-access corners. Not everything is same-old, same-old though: the new 'Artemis' in-the-cloud detection layer which has been attracting much attention in recent months, is apparently rolled into this version, as shown by a button offering additional online heuristic data. As this was disabled by default, its input did not count towards detection scores under the VB100 rules.

On-demand speeds were reasonable, on-access overheads a little heavy, with executable files particularly slow to process, and detection rates proved pretty solid, with a gradual decline across the RAP weeks to a fairly steep drop in the 'Week+1' set. The new Virut strain was not quite fully covered with a single item missed, but the WildList presented no problems and with the clean sets free from upset too, *McAfee* takes away another VB100 award.

MWTI eScan Internet Security for Windows 10.0.977.411

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	88.67%
Worms & bots	100.00%	**False positives**	0



MicroWorld's *eScan* has a rather cuddly, cartoony feel to it in places but retains an air of solidity and thoroughness nevertheless. Set-up is a breeze, but once finalized the main interface did seem rather reluctant to show itself, on occasion taking as long as 20 seconds from click to full display. There were a few similarly long lags accessing logs at times too, mostly thanks to their large

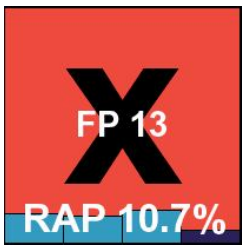
File access lag time (s/MB)	Archive files				Binaries and system files				Media and documents				Other file types			
	Default settings		All files		Default settings		All files		Default settings		All files		Default settings		All files	
	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)	Time (s)	Lag (s/MB)
Agnitum Outpost	67	0.02	NA	NA	464	0.17	464	0.17	163	0.07	163	0.07	107	0.09	107	0.09
AhnLab V3Net	82	0.03	NA	NA	222	0.08	222	0.08	113	0.04	113	0.04	100	0.09	100	0.09
Alwil avast!	142	0.05	562	0.19	272	0.10	292	0.11	194	0.08	219	0.09	165	0.16	171	0.16
AVG Internet Security	228	0.07	238	0.08	387	0.14	388	0.14	108	0.04	133	0.05	33	0.01	65	0.05
Avira AntiVir	44	0.01	172	0.06	194	0.07	194	0.07	110	0.04	150	0.06	55	0.04	146	0.14
BitDefender Security	581	0.19	1469	0.49	320	0.12	342	0.13	105	0.04	119	0.05	105	0.09	109	0.10
CA eTrust	27	0.01	NA	NA	66	0.02	66	0.02	65	0.02	65	0.02	43	0.03	43	0.03
ESET NOD32	12	0.00	NA	NA	61	0.02	61	0.02	75	0.03	75	0.03	56	0.04	56	0.04
Fortinet FortiClient	277	0.09	277	0.09	350	0.13	350	0.13	63	0.02	63	0.02	74	0.06	74	NA
Frisk F-PROT	71	0.02	NA	NA	323	0.12	323	0.12	52	0.01	52	0.01	43	0.03	43	0.03
F-Secure Anti-Virus	52	0.02	1670	0.55	370	0.14	423	0.16	150	0.06	223	0.10	148	0.14	224	0.22
K7 Total Security	76	0.02	NA	NA	250	0.09	250	0.09	57	0.02	57	0.02	52	0.04	52	0.04
Kaspersky Anti-Virus	376	0.12	1427	0.47	350	0.13	376	0.14	186	0.08	211	0.09	159	0.15	181	0.17
McAfee VirusScan	41	0.01	497	0.16	488	0.18	814	0.31	101	0.04	114	0.04	108	0.10	118	0.11
MWTI eScan	358	0.12	496	0.16	232	0.08	232	0.08	61	0.02	72	0.02	55	0.04	86	0.07
Netgate Spy Emergency	48	0.01	NA	NA	108	0.04	NA	NA	105	0.04	NA	NA	41	0.02	NA	NA
Norman Virus Control	44	0.01	NA	NA	207	0.07	207	0.07	94	0.03	94	0.03	103	0.09	103	0.09
Quick Heal Anti-Virus	15	0.00	NA	NA	66	0.02	NA	NA	65	0.02	NA	NA	29	0.01	NA	NA
Sophos Anti-Virus	63	0.02	1124	0.37	463	0.17	483	0.18	141	0.06	182	0.08	160	0.15	190	0.18
Symantec Endpoint Protection	37	0.01	NA	NA	228	0.08	228	0.08	163	0.07	163	0.07	142	0.13	142	0.13
TrustPort Antivirus	301	0.10	NA	NA	593	0.22	593	0.22	194	0.08	194	0.08	188	0.18	188	0.18
VirusBuster Professional	24	0.01	29	0.01	177	0.06	175	0.06	47	0.01	94	0.03	30	0.01	64	0.05

size after scanning large infected sets, but otherwise things were smooth and reliable. On-demand scanning speeds were very slow, but on access speeds were around the middle of the field. Detection rates were pretty good, with a very slow decline in the RAP sets and an excellent showing in the 'Week+1' set, as well as flawless coverage of the polymorphic sets. With no untoward issues in the WildList or clean sets, *eScan* comfortably wins a VB100 award.

Netgate Spy Emergency 2009 6.0.305.0

ItW	69.96%	**Polymorphic**	1.77%
ItW (o/a)	69.96%	**Trojans**	14.56%
Worms & bots	77.33%	**False positives**	13

A newcomer to the VB100 this month, *Netgate*'s *Spy Emergency* suffers from a rather improbable name with more than a hint of the rogue product about it. The product itself provides a very slick and professional installation and set-up process however, dented in seriousness only by the option to select the GUI skin colour at the end. The interface itself is also attractive and well designed, with only a minimum level of configuration, but what controls there are proved responsive. Logging proved a little less reliable, possibly thanks to inept user interaction, but nevertheless



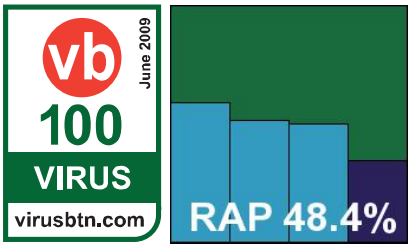
Archive scanning		ACE	CAB	EXE	JAR	LZH	RAR
Agnitum Outpost	OD	2	√	√	√	X	√
	OA	X	X	X	X	X	X
AhnLab V3Net	OD	9	9	9	9	9	9
	OA	X	X	X	X	X	X
Alwil avast!	OD	X/√	X/√	√	X/√	X/	X/√
	OA	X/	X/√	√	X/√	X/	X/√
Avira AntiVir	OD	√	√	√	√	√	√
	OA	X	X/	X/√	X/√	X/	X/√
AVG Internet Security	OD	X	√	√	√	√	√
	OA	X	X	X	X	X	X
BitDefender Security	OD	√	√	8	√	√	√
	OA	X/8	X/8	X/4	8	X/8	X/8
CA eTrust	OD	X	√	√	√	√	√
	OA	X	X	X	1	X	X
ESET NOD32	OD	√	√	√	√	√	√
	OA	X	X	X	X	X	X
Fortinet FortiClient	OD	X	√	√	√	√	√
	OA	X	√		√		√
Frisk F-PROT	OD	1	√	√	√	√	√
	OA	1	X	2	2	X	X
F-Secure Anti-Virus	OD	X/√	5	5	5	5	5
	OA	X/√	X/5	X/5	X/5	X/5	X/5
K7 Total Security	OD	X	1	X	1	1	1
	OA	X	X	X	X	X	X
Kaspersky Anti-Virus	OD	√	√	√	√	√	√
	OA	X/	X/√	√	X/√	X/	X/√
McAfee VirusScan	OD	X/2	X/	X/√	X/√	X/	X/√
	OA	X/2	X/	X/	X/√	X/	X/
MWTI eScan	OD	√	√	8	√	√	√
	OA	X/	X/√	X/8		X/√	X/√
Netgate Spy Emergency	OD	X	X	X	X	X	X
	OA	X	X	X	X	X	X
Norman Virus Control	OD	X	X	√	√	√	√
	OA	X	X	X	X	X	X
Quick Heal Anti-Virus	OD	X/2	X/5	X	X/5	X	X/5
	OA	X	X	X	X	X	X
Sophos Anti-Virus	OD	X	X/5	X/5	X/5	X/5	X/5
	OA	X	X/5	X/5	X/5	X/5	X/5
Symantec Endpoint Protection	OD	X	3/	3/√	3/	3/	3/√
	OA	X	X	X	X	X	X
TrustPort Antivirus	OD	X	√	√	√	√	√
	OA	X	X	X	X	X	X
VirusBuster Professional	OD	2	√	√	X	X	√
	OA	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

numerous pop-up alerts failed to be recorded in initial attempts. When full detection data was finally gleaned, coverage of the sets was fairly poor, with large numbers missed in the WildList set. False positives were also an issue, with handfuls of false alarms in several of the sets, most notably a selection of samples taken from clean *Windows 98* installs, including notepad.exe, calc.exe and explorer.exe. Polymorphic detection was also fairly poor, with very few samples detected at all and no single variant fully covered. There is clearly a good deal of work to be done here before the product is ready for VB100 certification, but it seems like a decent start has been made and those hints of roguishness implied by the unfortunate title should soon be dispelled.

Norman Virus Control 5.99

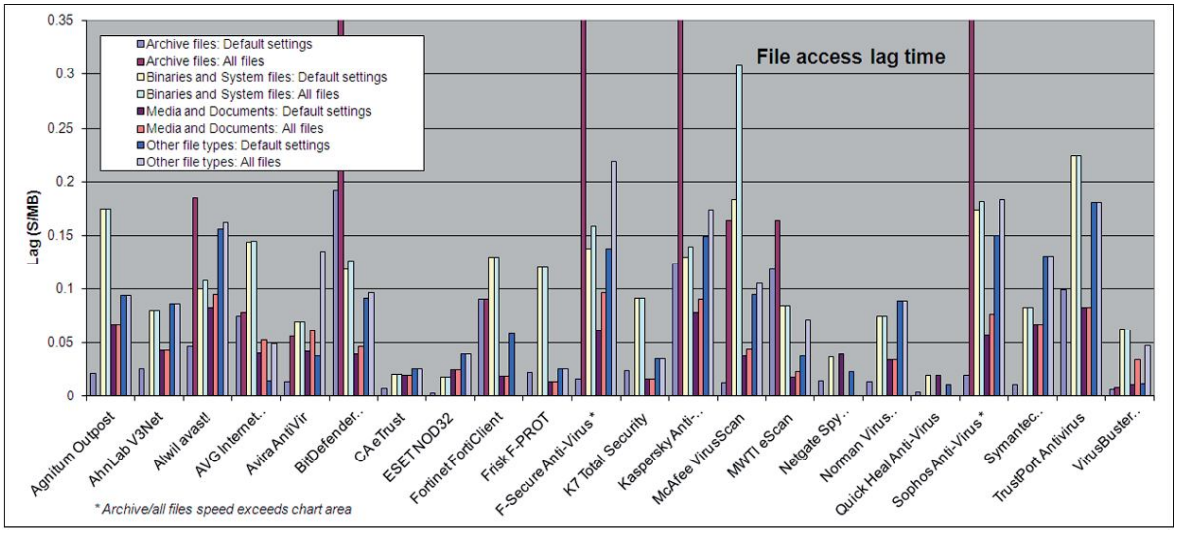
ItW	100.00%
ItW (o/a)	100.00%
Worms & bots	100.00%
Polymorphic	83.19%
Trojans	71.99%
False positives	0

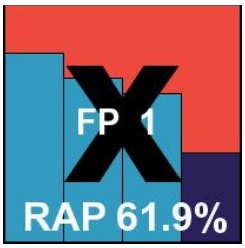


Norman's installation is simpler than most: a bare *InstallShield*-style process trips through the standard steps and ends, after suggesting that a reboot may be required, with no call for one. The *VC* control system is a rather fiddly, multi-interface system which requires several different windows to design and initiate a scan – however, with the benefit of some familiarity, it presented no serious problems. A few irritations included the absence of some options that would have been useful, some options not seeming to work, and despite explicitly setting all actions to log only, numerous samples were removed or disinfected in the various scans run. Scanning speeds and overheads were mostly fairly good, although the executable speed test set took quite some time on demand, and results were fair to middling across the various sets, with some issues apparent over the new Virut samples. The Wildlist presented no such problems however, and with no false positives either *Norman* earns a VB100 award.

Quick Heal Anti-Virus Lite 2009 10.00

ItW	100.00%	**Polymorphic**	95.69%
ItW (o/a)	100.00%	**Trojans**	87.95%
Worms & bots	99.77%	**False positives**	1



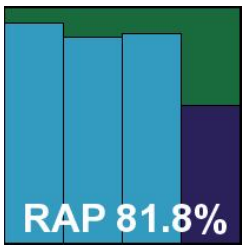


Quick Heal continues to live up to its name, providing a rapid and simple installation to go with its fast, uncomplicated product. The latest version of the interface has a crisp, clean glow about it that is very easy on the eye, and the layout remains basic but highly usable. An absence of in-depth options may put off more demanding admins, and some other issues emerged, including an apparent inability to save on-access logs and a tendency to ignore instructions not to interfere with any infections discovered. Also rather frustrating was a lengthy delay accessing browse windows when selecting targets for on-demand scans, sometimes taking over half a minute to display the filesystem. With this hurdle overcome, scanning speeds and overheads were most impressive.

Detection was also very good, with an excellent showing in the trojans set, full coverage of all our Virut samples, and a decent performance in the RAP set-up too. With the WildList presenting no problems, only the clean sets remained an obstacle to VB100 certification, and here sadly the same browser product which tripped up another product earlier was alerted on, using the same identification – suggesting some contamination of shared sample sets somewhere – and *Quick Heal* also misses out on a VB100 award by a whisker.

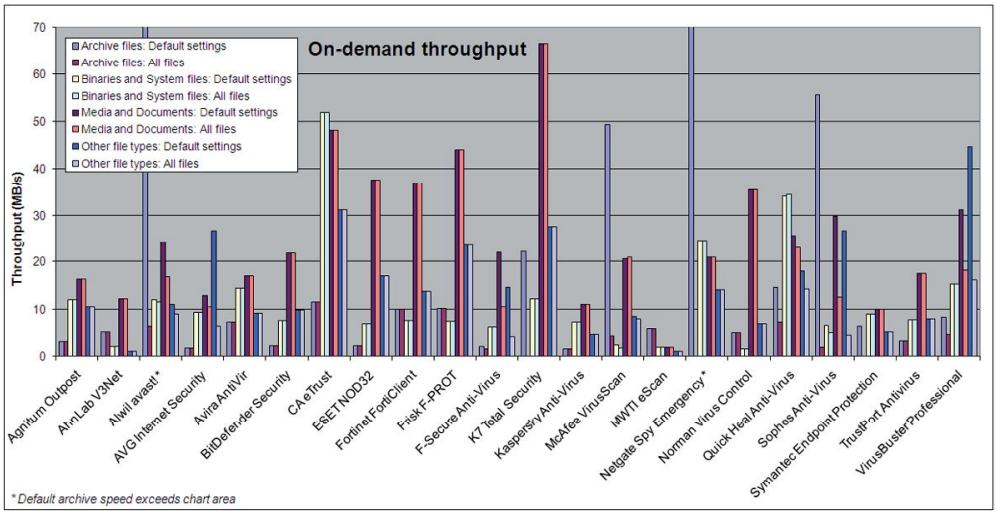
Sophos Anti-Virus 7.6.6

ItW	100.00%	**Polymorphic**	99.97%
ItW (o/a)	100.00%	**Trojans**	88.90%
Worms & bots	100.00%	**False positives**	0



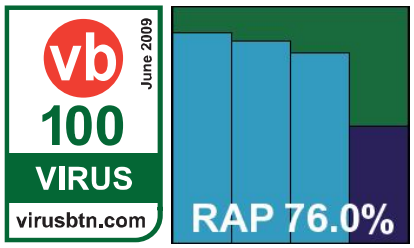
Sophos's set-up procedure starts with a simple unzipping and leads through the standard stages, via an offer to remove competitors' software and a couple of command prompt windows which flicker up briefly, to full activation in short order, with no reboot required. The interface looks much as it has done for some time: a fairly plain and bare look with a splendidly complete range of configuration options available beneath the surface, including a highly advanced area where interference without expert guidance is strongly discouraged.

Initial attempts at the speed tests found that on-demand scans invariably included additional scanning for rootkits and suspicious files in standard areas. This added several minutes to each scan, even over a small handful of files, so tests were redone using the right-click option to more closely approximate the standards set elsewhere. The progress bar remains worse than useless, invariably shooting to 80% in the first few minutes of a scan and lingering there for most of the remainder, be that five minutes or 90, but several other products also had some issues in this area. In the final reckoning, scanning speeds were very good, on-access overheads a little heavy, but detection rates were really quite excellent across the board, with a commendably stable set of figures across the trojans and first three weeks of the RAP sets. The WildList was handled easily, and while a sprinkling of items in the clean sets were labelled vaguely suspicious, this is permissible within the VB100 rules and *Sophos* wins another VB100 award.



Symantec Endpoint Protection 11.0.4010.19

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.59%
Worms & bots	100.00%	**False positives**	0

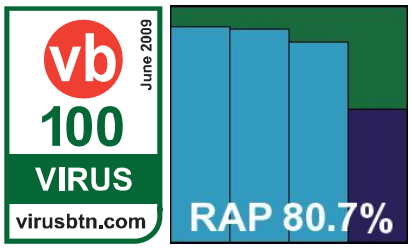


Symantec's corporate product provides options for central or local management to kick off its installation. We opted for local controls, and the rest of the set-up followed the usual path, although when it reached the end and suggested it would require 'several minutes' to tidy up after itself, it was something of a surprise to find that it actually meant it. A reboot was then required, after an attempt to update. The latest interface is a bright and shiny thing, not unpleasant to look at and providing a fair degree of configuration options in its more advanced regions (although some items we looked for were not available). The product includes some additional 'proactive' protection mechanisms, but these were disabled by default.

The system for designing and running on-demand scans proved pleasingly simple and quick to respond, and the bulk of the tests were handled with ease, producing somewhat below-par speeds in both modes but decent detection rates in most sets. These last figures were obtained only with great patience, as scanning large numbers of infected files takes some time – fortunately not a situation most admins would expect to encounter. Logging also proved rather fiddly, with the product taking an enormous amount of time to display and export logs, which in some cases seemed incomplete. Once data was finally accessed, a single sample of the latest Virut strain proved not to have been detected but the WildList was covered with ease. With no false positives either, *Symantec* earns another VB100 award.

TrustPort Antivirus 2009 2.8.0.3014

ItW	100.00%	**Polymorphic**	98.82%
ItW (o/a)	100.00%	**Trojans**	83.63%
Worms & bots	100.00%	**False positives**	0

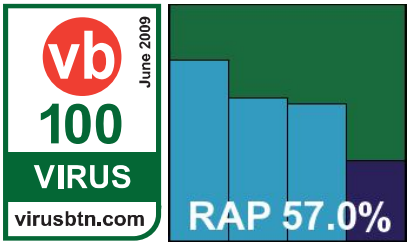


TrustPort is another product to have had something of a facelift of late, with a curvaceous new company logo, some new fonts and a new colour scheme enlivening what is essentially a very similar layout to earlier versions. The installation process includes a strongly worded warning about installing on machines running other security products, and has a post-install configuration scheme including options to control the order in which the two engines included are applied. The interface is available as a highly simplified version, or as a more advanced one. This does indeed provide an advanced level of configuration, although once again some options were clearly absent, and indeed one – the choice to scan compressed files on access – seemed to have little effect when activated. A few other small worries were encountered, most notably some slow startup times for the on-access protection, which seemed still not to be working long after the newly booted machine was responding to commands. On one occasion a scan came to a halt with the stark message that an API error had occurred. Scanning speeds were rather slow, as one would expect from

a multi-engine product, but detection rates were generally very good, although a worryingly large number of new Virut samples were not flagged. There were no problems in the WildList or elsewhere, and *TrustPort* thus also earns a VB100 award.

VirusBuster Professional for Windows Servers (x64) 6.1.130

ItW	100.00%	**Polymorphic**	88.58%
ItW (o/a)	100.00%	**Trojans**	80.25%
Worms & bots	99.91%	**False positives**	0



Bringing up the rear of the alphabetical product list as usual, *VirusBuster*'s server edition presents a rather confusing mix of the desktop and server approach. The installation process is fairly simple, and when up and running an interface can be accessed from the system tray and looks very similar to the standard desktop GUI. A brief browse through it, however, revealed that several standard options, and indeed sets of options, are not available here. To find them, one must turn to a second, MMC-based console, for which a shortcut is dropped onto the desktop. This made for some slightly odd flipping between the two as different tweaks needed to be made in various places. Occasionally some slow response times also frustrated, particularly when adjusting the targets of a scan, with long pauses after each stage of the set-up process. Finally, an issue which has been noted here several times before: the option to enable on-access scanning of archives is provided but appears entirely ineffectual.

Despite these minor irritants, scanning speeds were excellent and detection rates not bad at all, although as with so many other products this month, some work may need to be done on the latest W32/Virut strain. For now, however, the WildList set presented no issues, and without false positives either *VirusBuster* earns another VB100 award.

CONCLUSIONS

As expected, the 64-bit platform brought out quite a number of quirks and oddities in several of the products under test. While last month's comparative suffered from a rash of severe stability issues, with systems freezing and crashing all over the place, this kind of problem was less evident this time, although not completely absent. This is to be expected, as server products do generally need to be more resilient, and crashing a server system is a big sin for any software. However, this month's batch of products showed some more insidious problems, with logging inaccuracies, settings seeming to readjust themselves in some products, while in others they were simply ignored. These are also pretty big crimes in a server system, where admins expect their security software to conform to their requirements and not go off doing its own thing. We have emphasized the availability (or otherwise) of configuration options and fine-tuning controls throughout this month's review, as this is an important aspect of products in a server setting – some of the products proved somewhat lacking in this area.

Detection also seemed a little uneven in some products, with oddly differing behaviour in different modes. Some products did not perform as well as previous experience led us to expect, much of which can be put down to the complexities of the platform and the fact that many developers seem to put more effort into desktop and home-user solutions than into server products. Thanks to this, the RAP results have yet to settle down and show any steady patterns across the board, but after three outings some top performers are starting to emerge, while the rest jostle for position below them.

Since the last test we have been doing some filtering of our clean sets to ensure the most obscure and improbable items are removed. Many of these, including several previously alerted on as false alarms, have been kept handy in a side-set and monitored during testing. This has shown an increasing trend of false alarms spreading across the industry, as clean items make their way into sample collections and are blindly added to detection databases by automated systems. This is perhaps an inevitable side effect of the increased use of such automation, but is a danger labs need to be alert to and should mitigate as best they can.

Of the products failing this month, most were fairly clear false positive issues, of which a few seemed to be shared between products; some products were unlucky with fairly minor false alarms, while the lone newcomer, with a more sizeable clutch of false positives, was expected to have some teething issues and will doubtless improve rapidly. The WildList was handled fairly easily, but next time it should present a much tougher challenge, with the latest W32/Virut strain almost certain to stay in the list long enough to make the next test set and still proving to cause difficulties several months after it was first observed.

Technical details

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 2003 Server R2 SP2*, x64 edition.