COMPARATIVE REVIEW

WINDOWS SERVER 2003

John Hawes

While *VB*'s past comparative reviews on server platforms have generally been less heavily subscribed than desktop tests, this month sees the continuation of the recent upward trend in the number of products taking part, with a total of 27 products on the test bench. While some vendors submitted dedicated server, or at least business-oriented versions of their products, several entries comprised much the same products as appear in desktop platform tests, which should be assumed to work perfectly well in the *Server 2003* environment.

With time pressing (a post holiday season illness meaning things got under way even later than originally planned), I could only hope for simple installation procedures, easily navigated configuration systems and solid, stable operation. Past experience has, of course, taught me that this was a little too much to hope for, but I went into the lab with my fingers crossed.

PLATFORM AND TEST SETS

Windows Server 2003 bears great similarity to *XP* (on which it is based) – with a number of adjustments to the default settings providing a little extra security – and the process of setting up the test systems presented few difficulties.

The deadline for product submission was the first Monday of the year, 7 January, with the content of the test sets frozen the preceding Friday. Rather hasty pre-Christmas preparations for the review meant that my usual check of significant calendar events was omitted, and the product submission deadline coincided unwittingly with Russian Orthodox Christmas celebrations and Christmas in some other areas, but vendors based in these territories still managed to get their products in without too much grumbling.

The test sets were based on the November issue of the WildList (released in mid-December), which included a fairly standard number of additions heavily dominated by worms with familiar names, or at least behaviours. There were once again a handful of polymorphic file-infectors, including several of the W32/Virut variants which caused such mayhem in the last test. A fairly large number of items also fell from the list and were thus relegated to other test sets.

These other sets were subject to minimal updating, due to the shortage of time for preparations, and the clean set was also expanded in only a minor way, with a few dozen packages and their contents added. With limited changes from the test sets used in the last round of testing, I hoped for considerably better performance from the products this time around.

In addition to testing basic detection performance, we have once again included tests of the products' archive scanning depth, both in default settings and with more complex scanning options enabled. Only products which could be cajoled into detecting the EICAR test sample hidden three levels deep in archives are included in the tables for these sets, and only those spotting the test string in a file with a randomly selected extension appear on the 'all files' tables (although in some cases this only indicates that products are getting file type information from within files rather than simply from the extension, and full scanning may not always be occurring). We hope that the data provides some insight into the efficiency of the products under test.

AEC Trustport Antivirus 2.8.0.1628

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	3

AEC's *Trustport* suite contains a number of items beyond the anti-virus component, but as usual only this module was submitted for testing. This made installation a pretty straightforward process, and left me with no main interface from which to operate – configuration and functions are instead accessed from a system tray menu. The default settings are pretty thorough, detecting everything in our archive and file-extension scanning test set, and combined with the multi-engine layout this led to some rather languid scanning times.

AEC's entry in the last comparative review (see *VB*, December 2007, p.16), its first since the *BitDefender* engine was dropped from the product in favour of those of *Dr.Web* and *VirusBlokAda*, suffered from some false positive issues as well as several WildList misses. Detection was greatly improved this time, with nothing at all missed on demand, and only a few older items missed on access (where not all the available engines are used by default). However, despite one of the engines apparently being disabled entirely, and greyed out in configuration dialogs, several false positives were recorded, which once again deny *AEC* a VB100 award.

Agnitum Outpost Security Suite Pro 6.0.2227.232.0465

ItW	99.80%	**Worms & bots**	99.91%
ItW (o/a)	99.80%	**DOS**	99.77%
File infector	99.21%	**Macro**	100.00%
Polymorphic	85.91%	**False positives**	0

Agnitum's *Outpost* was subject to an in-depth review last month (see *VB*, January 2008, p.17), after achieving its first VB100 certification in the previous comparative. With the review still fresh in my mind, the installation process and configuration were fairly straightforward, although the product is sufficiently well designed to present few difficulties for those without any prior knowledge.

The available configuration is somewhat limited, with no option to scan archives in on-access mode, but other files did seem to be inspected regardless of their extension, and speeds were fairly reasonable considering. False positives were entirely absent, and detection in most of the test sets at the pretty high level expected from the *VirusBuster* engine in use. In the WildList set, however, a single instance of a W32/VB worm was missed, as well as two samples of one of the new W32/Virut variants. This presaged problems for some of the products further down the list using the same technology, and meant *Agnitum* didn't quite manage to add to its VB100 tally.

AhnLab V3Net for Windows Server 6.1.21.711

ItW	100.00%	**Worms & bots**	99.70%
ItW (o/a)	100.00%	**DOS**	97.18%
File infector	98.95%	**Macro**	98.99%
Polymorphic	92.88%	**False positives**	0

AhnLab has not been a regular participant in VB100 tests recently, but the AVAR conference the company hosted in Seoul a few weeks before the test deadline provided an opportunity to pester the developers into joining in again – an effort which paid off with this entry.

The *V3Net* product is quick and easy to install and set up, with a clear and pleasant interface adorned with a touch of cartoonishness without seeming too silly. The configuration is a little lacking on access, with no option to delve inside archives in this mode – something which seemed a little odd in a dedicated server product, as one might expect experienced admins to be interested in having a fuller range of options available. Even in on-demand mode, where most archive types were examined quite deeply, self-extracting executables and installer files were omitted. Another oddity which may cause admins frustration is the format of logs, which record only filenames with no information as to where the files in question may be found – this made for considerably more work in processing the test results.

Detection itself was less of an issue. No false positives were recorded and, despite a handful of misses in some of the older test sets, nothing significant was missed in the WildList set, thus *AhnLab* earns a VB100 award on its return to the test bench.

Alwil avast! Server Edition 4.7.865

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	98.67%
File infector	100.00%	**Macro**	99.98%
Polymorphic	86.99%	**False positives**	0

The server version of *avast!* seems little different from the standard version, or at least from the 'enhanced' interface usually necessary for the VB100 test. All the required configuration was readily available, with the defaults set not to scan archives internally but options available to scan the full range of archive types included in our test sets. Oddly, the renamed version of the EICAR test file was spotted on access but not on demand, implying that the on-access scanner is set up a little more thoroughly than the normally more in-depth manual scans.

Speeds were impressive, and still fairly decent with the more complete scanning options enabled. Detection levels were reasonable across the sets, with nothing at all missed in the WildList set. With no false positives either, *Alwil* wins another VB100 award.

Avira AntiVir Server 8.00.00.1547

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.87%	**False positives**	0

Despite an installation process which seemed very familiar, after the required reboot *AntiVir*'s *Server* edition displayed significant differences from the desktop variant, with an MMC-based console provided for most of the required configuration options. The interface was not as simple to navigate and use as *Avira*'s desktop range, but seems to provide a pretty thorough range of controls for the administrator. On-access scanning was fairly straightforward, and thorough once fuller scanning was enabled, although a few files compressed with the ACE algorithm were missed despite more deeply nested samples of the same format being detected.

Some very good speeds were recorded in both modes, although the actual setup and running of on-demand scans

On-demand tests	WildList		Worms and bots		DOS		File infectors		Macro		Polymorphic		Clean sets	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	FP	Susp.
AEC Trustport	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	3	
Agnitum Outpost	3	99.80%	2	99.91%	20	99.77%	8	99.21%	0	100.00%	220	85.91%		
AhnLab V3Net	0	100.00%	5	99.70%	656	97.18%	2	98.95%	46	98.99%	544	92.88%		
Alwil avast!	0	100.00%	0	100.00%	1022	98.67%	0	100.00%	1	99.98%	664	86.99%		
Avira AntiVir	0	100.00%	0	100.00%	32	99.78%	0	100.00%	0	100.00%	3	99.87%		
BitDefender Security	0	100.00%	0	100.00%	8	99.78%	2	98.95%	3	99.93%	0	100.00%		2
CA eTrust	0	100.00%	0	100.00%	235	99.67%	1	99.74%	12	99.82%	9	99.64%		
Doctor Web Dr.Web	4	99.28%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		9
ESET NOD32	0	100.00%	0	100.00%	500	99.78%	0	100.00%	0	100.00%	0	100.00%		
Fortinet Forticlient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%		
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.97%		3
Grisoft AVG	0	100.00%	2	99.91%	197	99.10%	7	98.43%	0	100.00%	695	78.55%		
Ikarus Virus Utilities	37	99.55%	4	99.60%	2460	91.37%	19	96.28%	151	96.45%	365	82.05%	8	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.97%		
Kingsoft Anti-virus	19	99.26%	639	16.85%	14050	12.26%	114	71.83%	355	91.56%	2020	38.49%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront	0	100.00%	0	100.00%	0	100.00%	1	99.90%	0	100.00%	80	96.46%		
MWTI eScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.97%		2
Norman Virus Control	4	99.95%	0	100.00%	269	99.12%	7	99.15%	0	100.00%	706	84.20%	1	
PCTools AntiVirus	3	99.80%	2	99.91%	20	99.77%	8	99.21%	0	100.00%	220	85.91%		
Quick Heal AntiVirus Lite	0	100.00%	0	100.00%	1149	95.23%	17	97.64%	73	98.23%	1081	81.86%	5	
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.97%		2
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	0	100.00%		22
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
VirusBuster for Windows Servers	1	99.82%	2	99.91%	20	99.77%	8	99.21%	0	100.00%	220	85.91%		
Webroot SpySweeper with AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	6	99.93%	0	100.00%		3

took much more time, with a rather awkward and fiddly setup process, and no indication of scanning progress at all. Once the complexities of the design were cracked, scan results showed the product's usual excellent detection rates and no false positives, giving *Avira* another VB100 award.

BitDefender Security for Windows Server 2.4.227

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	98.95%	**Macro**	99.93%
Polymorphic	100.00%	**False positives**	0

BitDefender also provided a special server version for this test, again incorporating a console interface using the MMC framework. This seemed rather more logically laid out and took less effort to decipher, but also seemed to be missing some useful options. The on-access scanner, for example, seemed to offer no option to block access only, making this action available only after attempts at other 'cleaning' methods had failed. This resulted in my test collection being trashed and requiring restoration between tests. Another apparent failing was an issue with setting up on-demand scans. Assuming at first that these could again only be run from the scheduler, I set up a scan using the default time offered, which was in fact the current time – ideal for my needs. However, by the time the setup process had finished, the moment had passed and the scan thus failed to initiate, waiting instead for the same time to roll around the following day. My frustration was quickly sidestepped when I found the proper place to run manual scans, with a 'scan now' option available.

Having deciphered the interface, testing continued without further stumbles, with fairly good speeds and the default settings covering most file types in depth. Detection was pretty close to flawless across the test sets including the WildList, and in the clean sets a few items were flagged as adware but no false positives were recorded, granting *BitDefender* a VB100 award.

CA eTrust Antivirus 8.1.6370

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.67%
File infector	99.74%	**Macro**	99.82%
Polymorphic	99.64%	**False positives**	0

CA's *eTrust* is a corporate-focused product, and has been submitted in much the same form for just about all VB100 tests I have run. This month was no different, and the familiar interface, its frustrations of slow connection times slightly less intrusive than usual, powered through the tests in splendid time. On-access archive scanning appeared to be absent, despite a number of options relating to such scanning being activated – single-level zip and jar archives were penetrated in this mode, but no other types or greater depths. On-demand scanning proved more thorough, although ACE and self-extracting EXEs were only probed one level deep.

Detection levels were very high, with almost complete coverage across the test sets and the WildList covered without difficulty. Without false positives *CA* easily makes the grade required for a VB100 award.

Doctor Web Dr.Web Antivirus for Windows Server 4.44.1.01090

ItW	99.28%	**Worms & bots**	100.00%
ItW (o/a)	99.28%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Doctor Web's product presented the same slick and solid design which impressed me in the last test, although the rather basic font used in the installer looks slightly out of place in its glossy surroundings. The clear layout of the interface made testing smooth and problem-free, with sensible defaults and deep configuration available. A few times on shutting down the on-access scanner there were error messages that claimed there were issues with disabling the protection, but it certainly seemed to have closed properly and restarted without further problems.

Scanning speeds were excellent, particularly in the default mode, which uses a 'smart' setting to determine which files are worth scanning. With thorough scanning of all files enabled things slowed down somewhat, but detection was pretty good across the board, with no more than a few files missed in each set, most of them down to file types not scanned by default. No false positives were in evidence, but unfortunately for *Doctor Web* a few items added to the latest WildList were not covered, and the VB100 award remains just out of reach.

ESET NOD32 Antivirus 3.0.621.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	99.78%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

On-access tests	WildList		Worms and bots		DOS		File infectors		Macro		Polymorphic		Clean sets	
	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	No. missed	%	FP	Susp.
AEC Trustport	0	100.00%	0	100.00%	90	99.78%	0	100.00%	0	100.00%	553	90.61%	2	
Agnitum Outpost	3	99.80%	2	99.91%	20	99.77%	10	98.69%	0	100.00%	220	85.91%		
AhnLab V3Net	0	100.00%	5	99.70%	656	97.18%	4	98.95%	46	98.99%	544	92.88%		
Alwil avast!	0	100.00%	0	100.00%	1022	98.67%	0	100.00%	4	99.93%	664	86.99%		
Avira AntiVir	0	100.00%	0	100.00%	32	99.78%	0	100.00%	0	100.00%	3	99.87%		
BitDefender Security	0	100.00%	2	99.96%	8	99.78%	4	98.43%	1	99.98%	0	100.00%		2
CA eTrust	0	100.00%	0	100.00%	235	99.67%	3	99.21%	12	99.82%	9	99.64%		
Doctor Web Dr.Web	4	99.28%	2	99.72%	0	100.00%	2	99.48%	0	100.00%	0	100.00%		6
ESET NOD32	0	100.00%	0	100.00%	500	99.78%	0	100.00%	0	100.00%	0	100.00%		
Fortinet Forticlient	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Frisk F-PROT	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.95%		
F-Secure Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	1	99.97%		1
Grisoft AVG	0	100.00%	2	99.91%	197	99.10%	9	97.90%	3	99.93%	695	78.55%		
Ikarus Virus Utilities	37	99.55%	4	99.60%	2460	91.37%	19	96.28%	159	96.26%	365	82.05%	8	
Kaspersky Anti-Virus	0	100.00%	0	100.00%	0	100.00%	2	99.48%	0	100.00%	1	99.97%		
Kingsoft Anti-virus	19	99.26%	639	16.85%	14050	12.26%	114	71.83%	355	91.56%	2020	38.49%		
McAfee VirusScan	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
Microsoft Forefront	0	100.00%	0	100.00%	0	100.00%	3	99.38%	0	100.00%	80	96.46%		
MWTI eScan	0	100.00%	0	100.00%	2	100.00%	0	100.00%	0	100.00%	0	100.00%		2
Norman Virus Control	8	99.90%	0	100.00%	269	99.12%	9	98.62%	8	99.80%	865	79.21%	1	
PCTools AntiVirus	3	99.80%	2	99.91%	22	99.55%	10	98.69%	0	100.00%	220	85.91%		
Quick Heal AntiVirus Lite	0	100.00%	0	100.00%	1197	95.12%	20	96.72%	82	98.04%	1081	81.86%	5	
Redstone Redprotect	0	100.00%	0	100.00%	0	100.00%	2	99.48%	8	99.80%	0	100.00%		2
Sophos Anti-Virus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	8	99.80%	0	100.00%		22
Symantec Endpoint Protection	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%	0	100.00%		
VirusBuster for Windows Servers	1	99.82%	2	99.91%	20	99.77%	10	98.69%	0	100.00%	220	85.91%		
Webroot SpySweeper with AntiVirus	0	100.00%	0	100.00%	0	100.00%	0	100.00%	6	99.93%	0	100.00%		3

The latest incarnation of *ESET*'s product was reviewed on its release a few months ago (see *VB*, November 2007, p.19), and received some rather effusive praise for its stylish looks and smart design. As *NOD32* version 3 appeared on the VB100 test bench for the first time, the stylishness and clever layout continued to impress, allowing the tests to be run through with great simplicity and making the testing experience a joy.

Speeds were as excellent as ever, although probing into archives slowed things down somewhat, and this depth of scanning was not available on access – one of the only options notably absent. Detection could not be faulted in most sets, although a set of samples of an aged DOS polymorphic virus which caused no problems in previous tests were not detected with this version, returning an 'internal error' message in logs. This does not affect *NOD32*'s qualification for the VB100 award, which was achieved easily with full detection of the WildList set and no false positives.

Fortinet Forticlient 3.0.470

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Fortinet's product provided a similarly problem-free run through the tests. The installation, updating and configuration processes are familiar, the core interface having changed little for some time. The product is clearly laid out with all the required elements readily to hand, despite a wide range of other functionality (beside the anti-malware protection) being controlled from the same interface.

Little configuration was required, with the default settings including most file types. Somewhat oddly, ZIP files – perhaps the most common archive format – were scanned less deeply than others. This could be a resource-saving measure introduced due to the very popularity of the format. Despite the thoroughness speeds were quite impressive, and coverage of the sets excellent, with no misses and no false positives earning *Fortinet* a VB100 award.

Frisk F-PROT Antivirus for Windows 6.0.8.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.95%	**False positives**	0

F-Prot is a far simpler product than many, with a pared-down interface offering basic control of anti-malware protection and scanning, and little else. With minimal configuration available, and functionality such as logging generally excellently implemented, testing zipped through. Minimal configuration options cut the speed test requirements down, with only the product's seemingly unstoppable urge to remove infected files drawing out the process (an initial run was stopped and replaced with one in which detections were logged only after the first attempt proved to be spending considerable time disinfecting and quarantining).

Default archive settings were among the most sensible so far, with most archive types covered in depth on demand and the basics, self-extractors, ZIPs and the almost identical JAR files delved into a couple of levels deep on access. Speed times were splendid, and detection almost impeccable, earning *Frisk* a VB100 award too.

F-Secure Anti-Virus 7 for Windows Servers 7.00.213

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.97%	**False positives**	0

F-Secure's product is a little more complex and in-depth, though the server version tested here seems little different from the desktop editions seen in previous comparatives. The installation is slick and smooth, lending a solid and trustworthy feel to all components. This weightiness is not too evident in the scanning times, which were surprisingly good over most of the sets although, with the default setting to scan most archive types to a depth of five levels, this set took rather longer. Somewhat oddly next to this thorough setting, file types are identified only by extension, but scanning with 'all files' enabled did not take too much longer to complete, although an occasional moment of sluggishness was observed during operation of the machine thereafter.

F-Secure has presented me with considerable difficulty recently thanks to its rather flaky logging behaviour, which was in evidence once again here, with the 'display log' button bringing up an attractively formatted HTML log in a browser window. As in previous tests, the contents of this log varied wildly, apparently containing a random sampling of items discovered during a scan. Attempting to access the

On-demand throughput	Archive files - default		Archive files - all files		Binaries and system files - default		Binaries and system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - default	
	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Through-put (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)	Time (s)	Throughput (MB/s)
AEC Trustport	4965	0.8	4965	0.8	1677	1.6	1677	1.6	282	5.5	282	5.5	287	2.4	287	2.4
Agnitum Outpost	1185	3.3	1185	3.3	272	10.0	272	10.0	92	16.7	92	16.7	61	11.2	61	11.2
AhnLab V3Net	788	4.9	788	4.9	354	7.7	354	7.7	31	49.7	31	49.7	35	19.6	35	19.6
Alwil avast!	19	204.2	988	3.9	168	16.2	201	13.6	26	59.2	61	25.2	17	40.3	42	16.3
Avira AntiVir	738	5.3	738	5.3	114	23.9	114	23.9	32	48.1	32	48.1	25	27.4	25	27.4
BitDefender Security	1242	3.1	1242	3.1	322	8.5	322	8.5	71	21.7	71	21.7	73	9.4	73	9.4
CA eTrust	520	7.5	520	7.5	71	38.4	71	38.4	29	53.1	29	53.1	22	31.2	22	31.2
Doctor Web Dr.Web	4455	0.9	4455	0.9	756	3.6	756	3.6	102	15.1	102	15.1	108	6.3	108	6.3
ESET NOD32	1093	3.5	1093	3.5	432	6.3	432	6.3	33	46.7	33	46.7	27	25.4	27	25.4
Fortinet Forticlient	506	7.7	506	7.7	483	5.6	483	5.6	44	35.0	44	35.0	35	19.6	35	19.6
Frisk F-PROT	254	15.3	254	15.3	259	10.5	259	10.5	32	48.1	32	48.1	22	31.2	22	31.2
F-Secure Anti-Virus	3144	1.2	3375	1.1	254	10.7	254	10.7	39	39.5	89	17.3	25	27.4	93	7.4
Grisoft AVG	1379.2	2.8	1379.2	2.8	578.1	4.7	578.1	4.7	78.1	19.7	78.1	19.7	91.8	7.5	91.8	7.5
Ikarus Virus Utilities	211	18.4	211	18.4	206	13.2	206	13.2	40	38.5	50	30.8	59	11.6	61	11.2
Kaspersky Anti-Virus	287	13.5	287	13.5	149	18.3	149	18.3	94	16.4	94	16.4	87	7.9	87	7.9
Kingsoft Anti-virus	292	13.3	292	13.3	385	7.1	385	7.1	25	61.6	25	61.6	29	23.6	29	23.6
McAfee VirusScan	58	66.9	843	4.6	328	8.3	339	8.0	60	25.7	57	27.0	63	10.9	60	11.4
Microsoft Forefront	1190	3.3	1190	3.3	306	8.9	306	8.9	68	22.6	68	22.6	45	15.2	45	15.2
MWTI eScan	2314	1.7	2314	1.7	468	5.8	468	5.8	300	5.1	300	5.1	298	2.3	298	2.3
Norman Virus Control	807	4.8	807	4.8	1429	1.9	1429	1.9	53	29.0	53	29.0	153	4.5	153	4.5
PCTools AntiVirus	487	8.0	713	5.4	1115	2.4	1141	2.4	864	1.8	880	1.7	922	0.7	925	0.7
Quick Heal AntiVirus Lite	572	6.8	594	6.5	60	45.5	60	45.5	42	36.7	46	33.5	24	28.6	30	22.9
Redstone Redprotect	1863	2.1	1863	2.1	348	7.8	348	7.8	178	8.6	178	8.6	166	4.1	166	4.1
Sophos Anti-Virus	38	102.1	1446	2.7	210	13.0	260	10.5	29	53.1	48	32.1	15	45.7	58	11.8
Symantec Endpoint Protection	810	4.8	850	4.6	281	9.7	294	9.3	75	20.5	75	20.5	71	9.7	73	9.4
VirusBuster for Windows Servers	510	7.6	999	3.9	223	12.2	234	11.7	26	59.2	49	31.4	16	42.9	44	15.6
Webroot SpySweeper with AntiVirus	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

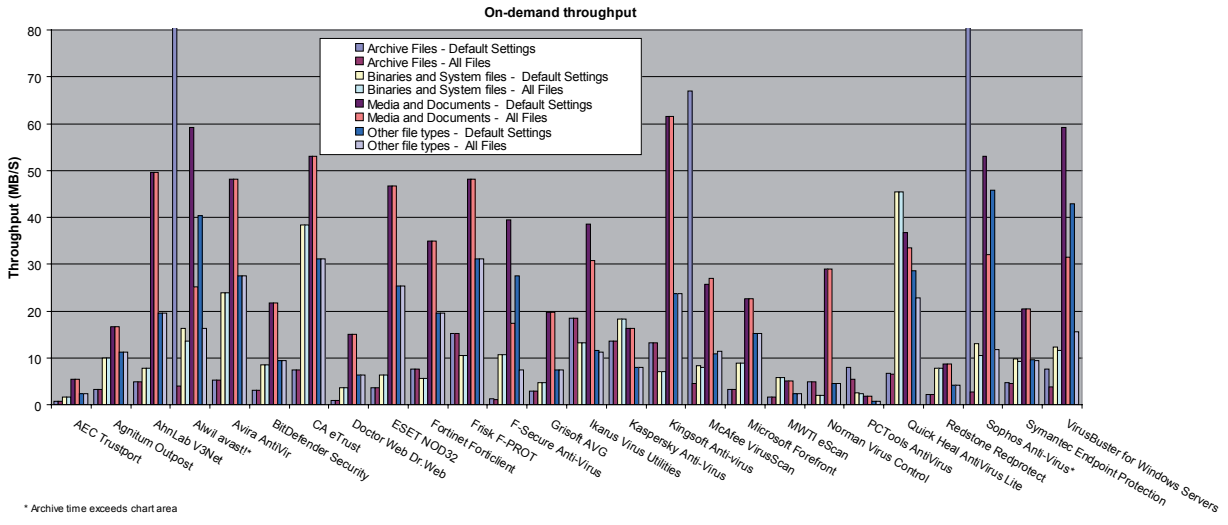
results of scanning the full test collection produced logs varying in size from 50 to 1500 KB. After much frustration trying to achieve the best results with this method, a series of smaller scans set to delete files proved the simplest way of judging the product's effectiveness.

This effectiveness was considerable, with splendid detection rates and no false positives, just a few alerts on suspect tools with potentially unwanted uses. With no problems at all in the WildList *F-Secure* also qualifies for a VB100 award.

Grisoft AVG 7.5.516

ItW	100.00%	**Worms & bots**	99.91%
ItW (o/a)	100.00%	**DOS**	99.10%
File infector	98.43%	**Macro**	100.00%
Polymorphic	78.55%	**False positives**	0

After an initial problem with an activation code inappropriate for use on a server, *AVG* proved somewhat



* Archive time exceeds chart area

simpler to handle, slipping slickly through its install and skipping lightly over the test sets. Although the multiple-window configuration system remains somewhat baffling, the limited configuration options were eventually tracked down and testing produced no major frustrations.

Scanning times were fairly decent, although again by default files with altered extensions are ignored. Detection rates were similarly solid rather than excellent, but the WildList was covered without difficulty, and with no false positives recorded *Grisoft* also makes the VB100 grade.

Ikarus Virus Utilities 1.0.61

ItW	99.55%	**Worms & bots**	99.60%
ItW (o/a)	99.55%	**DOS**	91.37%
File infector	96.28%	**Macro**	96.45%
Polymorphic	82.05%	**False positives**	8

Ikarus has bravely battered at the VB100 door for some time now, and has gradually moved closer to the required standard for qualification, with high levels of false positives having been the major stumbling block in recent tests.

The product's interface uses the .NET framework, and has suffered some flakiness in the past, which this month was considerably lessened. However, on a few occasions the GUI seemed to fail to open, and during the scanning of large infected sets the whole thing seems to flicker and spasm rather worryingly.

An initial run over the clean test set produced some remarkable speed times and an even more eyebrow-raising absence of false alarms. Some quick investigation quickly showed that I had omitted to apply the update, and that in its bare state the product has hardly any detection capabilities at all. Re-running the tests showed that a small number of clean files has been mislabelled, and a handful of WildList items missed, a few odd samples of several of the latest polymorphic additions. Although speed times were impressive and detection in the other sets fairly reasonable, *Ikarus* still has a few more issues to resolve before attaining a VB100 award.

Kaspersky Anti-Virus 6.0 for Windows Servers 6.0.3.837

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.97%	**False positives**	0

Kaspersky, meanwhile, is a seasoned competitor with a long history of excellent performance, a few minor technical issues in recent tests notwithstanding. The product, not quite as glossy and glitzy as the home-user offering provided lately, is no less solid or reliable for it, and offers a well-designed, intuitive interface with an excellent level of configuration, although scanning of archives on access seemed to produce a fairly erratic selection of depths for different formats.

After a few brief and easy tweaks the product stomped through the tests, speeds reflecting a more thorough attitude to scanning than many, but results showing splendid coverage and no false positives, thus earning *Kaspersky* yet another VB100 award.

File access lag time	Archive files - default		Archive files - all files		Binaries and system files - default		Binaries and system files - all files		Media & documents - default		Media & documents - all files		Other file types - default		Other file types - default	
	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)
AEC Trustport	1103	0.3	1103	0.3	476	0.2	476	0.2	117	0.1	117	0.1	145	0.2	145	0.2
Agnitum Outpost	64	0.0	N/A	N/A	293	0.1	293	0.1	95	0.1	95	0.1	75	0.1	75	0.1
AhnLab V3Net	77	0.0	N/A	N/A	355	0.1	355	0.1	37	0.0	37	0.0	40	0.0	40	0.0
Alwil avast!	96	0.0	1045	0.3	258	0.1	261	0.1	144	0.1	149	0.1	69	0.1	51	0.1
Avira AntiVir	35	0.0	284	0.1	118	0.0	141	0.0	31	0.0	42	0.0	19	0.0	47	0.1
BitDefender Security	927	0.2	927	0.2	364	0.1	364	0.1	150	0.1	150	0.1	147	0.2	147	0.2
CA eTrust	22	0.0	N/A	N/A	76	0.0	N/A	N/A	36	0.0	N/A	N/A	29	0.0	N/A	N/A
Doctor Web Dr.Web	7	0.0	3499	0.9	40	0.0	834	0.3	32	0.0	101	0.1	34	0.0	107	0.1
ESET NOD32	11	0.0	N/A	N/A	61	0.0	61	0.0	42	0.0	42	0.0	32	0.0	32	0.0
Fortinet Forticlient	385	0.1	385	0.1	478	0.2	478	0.2	38	0.0	38	0.0	47	0.1	47	0.1
Frisk F-PROT	70	0.0	N/A	N/A	251	0.1	251	0.1	40	0.0	40	0.0	25	0.0	25	0.0
F-Secure Anti-Virus	37	0.0	1819	0.5	222	0.1	370	0.1	44	0.0	249	0.2	28	0.0	114	0.2
Grisoft AVG	53	0.0	N/A	N/A	345	0.1	345	0.1	32	0.0	39	0.0	13	0.0	46	0.1
Ikarus Virus Utilities	214	0.1	214	0.1	218	0.1	218	0.1	52	0.0	52	0.0	71	0.1	71	0.1
Kaspersky Anti-Virus	34	0.0	232	0.1	203	0.1	289	0.1	76	0.0	133	0.1	49	0.1	119	0.2
Kingsoft Anti-virus	27	0.0	N/A	N/A	359	0.1	359	0.1	25	0.0	25	0.0	31	0.0	31	0.0
McAfee VirusScan	52	0.0	503	0.1	325	0.1	338	0.1	52	0.0	54	0.0	62	0.1	65	0.1
Microsoft Forefront	109	0.0	N/A	N/A	299	0.1	299	0.1	68	0.0	68	0.0	49	0.1	49	0.1
MWTI eScan	1162	0.3	1162	0.3	251	0.1	251	0.1	102	0.1	102	0.1	96	0.1	96	0.1
Norman Virus Control	22	0.0	N/A	N/A	226	0.1	226	0.1	58	0.0	58	0.0	77	0.1	77	0.1
PCTools AntiVirus	368	0.1	N/A	N/A	1036	0.4	N/A	N/A	144	0.1	N/A	N/A	110	0.1	N/A	N/A
Quick Heal AntiVirus Lite	12	0.0	N/A	N/A	58	0.0	N/A	N/A	36	0.0	N/A	N/A	15	0.0	N/A	N/A
Redstone Redprotect	3208	0.8	3208	0.8	299	0.1	299	0.1	127	0.1	127	0.1	121	0.2	121	0.2
Sophos Anti-Virus	40	0.0	1405	0.4	243	0.1	271	0.1	39	0.0	55	0.0	29	0.0	66	0.1
Symantec Endpoint Protection	29	0.0	N/A	N/A	200	0.1	200	0.1	41	0.0	41	0.0	38	0.0	38	0.0
VirusBuster for Windows Servers	34	0.0	N/A	N/A	225	0.1	226	0.1	31	0.0	50	0.0	18	0.0	43	0.0
Webroot SpySweeper with AntiVirus	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Kingsoft Anti-virus 2008.1.7.10

ItW	99.26%	**Worms & bots**	16.85%
ItW (o/a)	99.26%	**DOS**	12.26%
File infector	71.83%	**Macro**	91.56%
Polymorphic	38.49%	**False positives**	0

Kingsoft is another firm which has had some trouble in recent comparative reviews but has nevertheless continued to strive for the excellence required for a VB100 award. The company's product has grown in stability and responsiveness in the year or so since it first visited the *VB* test bench, and seems very pleasant to look at and rational to use.

Available configuration is less than complete but adequate for my needs, and testing trotted nicely along with impressive scanning times. False positives were pleasingly absent and detection rates showed further improvement,

but alongside a fair number of recent items in the older sets (including some quite significant W32/Sdbot and W32/Mytob variants), several worms in the WildList set were missed, as well as a few samples infected with W32/Virut and W32/Bacalid. As a result, a VB100 award still proves to be a little way out of reach for *Kingsoft* this month.

McAfee VirusScan Enterprise 8.5.0i 5200.2160

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

McAfee's enterprise product is a regular on the *VB* test bench and it took me little time to find my way around it. The layout is somewhat individual, but simple to operate and provides the full range of settings and controls expected in a complex corporate environment.

Adjusting the defaults to cover a wider range of file formats did not add too significantly to the pretty fair scanning times, although of course delving deeply into a broad range of archives was a little slower than leaving them unchecked.

The solidity of design and implementation was reflected in some effortlessly impressive detection rates, with nothing missed or mislabelled anywhere, and *McAfee* thus wins a VB100 award.

Microsoft Forefront Client Security 1.5.1941.0

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	99.90%	**Macro**	100.00%
Polymorphic	96.46%	**False positives**	0

Microsoft's product seems to take quite the reverse approach, assuming a mother-knows-best attitude and offering almost nothing by way of configuration options.

Rather amusingly, the installation process required an update to the Windows Update Agent before it could complete, and once installed the simple interface offered some basic information and a page of rather random controls.

The client in use here is part of a more complex suite of products, so it is possible that much of the configuration can be controlled from above. Nevertheless, it would seem appropriate to provide the user with a little more information on how their system is being monitored.

After running some scans and on-access tests a small amount of information emerged about how the product was operating, though little of this came from the product itself. After scanning several thousand infected files the GUI displayed the message 'Items Detected – Severe/High Alert level: 24', while all detections were logged only to the system event log once the on-screen display was closed. A 'History' button reopened the display from each scan, but regularly froze while trying to access the results of large scans and on occasion caused the whole interface to disappear from view.

Despite these annoyances, results were eventually dragged together and showed fairly good speeds. A sensible default selection of files handled all the archive sets without problem on demand and looked briefly into the most common types on access. Detection rates were very good indeed, and without any false positives *Forefront* is awarded a VB100.

MWTI eScan Corporate for Windows 9.0.764.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.97%	**False positives**	0

The corporate edition of *eScan* is a little more sober than the normal home desktop version, although its installation process with automatic scanning of important system areas remains much the same.

Configuration is provided via a console resembling the MMC, but dubbed 'EMC', and seems fairly comprehensive. However, little adjustment was needed as the default settings scanned pretty much everything thrown at it.

This resulted in some rather slow scanning speeds but of course excellent detection rates. A couple of items spotted as suspected malware by the *Kaspersky* engine in its other guises were missed here on access, and a few others that were not identified elsewhere were flagged here as potentially risky. However, with no samples missed in the WildList test set, and no false positives, *eScan* also qualifies for a VB100 award.

Norman Virus Control v.5.90.10

ItW	99.95%	**Worms & bots**	100.00%
ItW (o/a)	99.90%	**DOS**	99.12%
File infector	99.15%	**Macro**	100.00%
Polymorphic	84.20%	**False positives**	1

Norman's product is another which makes use of a variety of windows for various facets of its control and operation, and as usual this led to a certain amount of confusion and frustration. However, once their interoperation had been mastered things proceeded reasonably well, with the only issue found in the actual running of the product being a problem with the redirection of logs. An option to change the folder in which logs are saved seemed ideal for my use, but on checking the selected location at the end of the test it was found to be entirely log-free. Fortunately all the required data was stored within *Norman*'s own logging folder and results were thus gathered after only a brief moment of worry.

There was not a great deal of flexibility in the types of files scanned, with a handful of the more common archives investigated on demand but none on access. All file extensions were analysed for malicious content by default however, and this resulted in some rather below average speed times, as well as a single file in one of the clean sets being labelled as malware.

Detection rates were also less than perfect, with a handful of polymorphic variants in the WildList set not fully covered, the on-demand scanner faring slightly better than the on-access. *Norman* thus misses out on a VB100 award this month.

PCTools AntiVirus 3.6 for Windows 3.6.1.8

ItW	99.80%	**Worms & bots**	99.91%
ItW (o/a)	99.80%	**DOS**	99.77%
File infector	99.21%	**Macro**	100.00%
Polymorphic	85.91%	**False positives**	0

PCTools products have been a little awkward in the past, with an inflexibility of configuration providing some frustration. This time, however, everything I needed seemed to be both available and easily accessible. The installation offers an accompanying install of the *Google* toolbar, which I turned down for my tests, but few other difficult decisions were required.

Despite the default settings covering no archive types or renamed files on access, scanning speeds were on the slow side, and the system seemed less than usually responsive.

On-demand scans had slightly more thorough settings, with most archives probed to a single level, and the resulting speeds were even less impressive.

Scanning infected sets brought up a beautiful cascade of alert popups, scrolling and interweaving with each other down one side of the screen. Detection rates closely mirrored those of *Agnitum*, as both products use the *VirusBuster* engine, and thus it was hardly a surprise to see the same handful of misses in the WildList. Thus, despite a lack of false positives, *PCTools* does not receive a VB100 award for its efforts.

Quick Heal Quick Heal AntiVirus Lite 9.50

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	95.23%
File infector	97.64%	**Macro**	98.23%
Polymorphic	81.86%	**False positives**	5

Quick Heal is one of the few products to scan the system prior to installation, but the setup process is nevertheless speedy and efficient, offering a friendly 'Welcome' message flashing in the system tray. The interface is visually appealing and seems very stable and solid, but again configuration is kept to a minimum.

On-access settings can barely be adjusted at all, with no way of forcing files such as my renamed EICAR file to be watched for, and archives left unprobed. On-demand scanning is a little more thorough, with a few items delved into lightly by default and slightly more depth available for those who want it.

This lightness of scanning may contribute somewhat to the speed of the product, which was uniformly excellent. Detection rates were a little below average over the older sets but the WildList was covered without difficulty. In the clean set, a few items were incorrectly flagged as malicious, mostly identified as 'I-Worm.Sohanad.T', suggesting some overzealousness in the detection of this item. This inaccuracy is enough to deny *Quick Heal* a VB100 award this time.

Redstone Redprotect Anti-Virus Plus 0.4.2.1

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	99.97%	**False positives**	0

Redstone returns for a second attempt at the VB100, having been denied last time by a small technicality in the settings of the *Kaspersky* engine on which it is based. This

Archive scanning		ACE	CAB	EXEZIP	JAR	LZH	RAR	TGZ	ZIP	EXT*
AEC Trustport Antivirus	OD	X	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√
Agnitum Outpost	OD	X	√	√	X	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
AhnLab V3Net	OD	√	√	X	√	√	√	X	√	√
	OA	X	X	X	X	X	X	X	X	√
Alwil avast!	OD	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avira AntiVir	OD	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Security	OD	√	√	√	√	√	8	√	8	√
	OA	√	√	√	√	√	8	√	8	√
CA eTrust	OD	1	√	1	√	√	√	√	√	√
	OA	X	X	X	1	X	X	X	X	√
Doctor Web Dr.Web	OD	X	√	√	√	√	√	√	√	√
	OA	X	X/√	X/9	X/√	X/√	X/√	X/5	X/√	√
ESET NOD32	OD	X	√	√	√	√	√	X	√	√
	OA	X	X	X	X	X	X	X	X	√
Fortinet Forticlient	OD	X	√	√	√	√	√	√	4	√
	OA	X	√	√	√	√	√	√	4	√
Frisk F-PROT	OD	X	√	√	√	√	√	√	√	√
	OA	X	X	2	2	X	X	X	2	√
F-Secure Anti-Virus	OD	X/√	5	5	5	5	5	2	5	X/√
	OA	X/√	X/5	X/5	X/5	X/5	X/5	X/2	X/5	X/√
Grisoft AVG	OD	X	√	√	1	X	√	X	√	X
	OA	X	X	X	X	X	X	X	X	X/√
Ikarus Virus Utilities	OD	2	3	1	3	3	3	X	3	√
	OA	2	3	1	3	3	3	X	3	√
Kaspersky Anti-Virus	OD	√	√	√	√	√	√	√	√	√
	OA	X/4	X/4	X/1	X/4	X/5	X/5	X/1	X/2	√
Kingsoft Anti-virus	OD	X	X	X	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	√
McAfee VirusScan	OD	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/2	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Microsoft Forefront	OD	√	√	√	√	√	√	√	√	√
	OA	X	X	1	1	X	X	X	1	√
MWTI eScan	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Norman Virus Control	OD	X	X	X	√	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	√
PCTools AntiVirus	OD	1/2	1/√	1/√	1/√	X	1/√	X/√	1/√	√
	OA	X	X	X	X	X	X	X	X	X
Quick Heal AntiVirus Lite	OD	X	2/5	X	2/5	X	2/5	1	2/5	X/√
	OA	X	X	X	X	X	X	X	X	X
Redstone Redprotect	OD	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√
Sophos Anti-Virus	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
Symantec Endpoint Protection	OD	X	3/√	3/√	3/√	3/√	3/√	X/5	3/√	√
	OA	X	X	X	X	X	X	X	X	√
VirusBuster for Windows Servers	OD	2	√	√	X/√	X	√	√	√	X/√
	OA	X	X	X	X	X	X	X	X	X/√
Webroot SpySweeper with AntiVirus	OD	X	X	5	6	X	X	6	X	√
	OA	X	X	X	X	X	X	X	X	√

is another .NET product, again at a fairly early stage in its development, and some flakiness is evident in the running of the interface, with occasional unexpected shutdowns and the odd error message, particularly when trying to access

logs. Configuration is extremely minimal here, with the controls accessible from the system tray icon limited to running a scan and shutting down the on-access scanner. With the 'default' settings provided in the form of a series of registry keys it is here that adjustments must be made if needed – changing the default on-access behaviour (which seems to be to prompt users with a message offering not to delete if they respond within 30 seconds) seems not always to respond as expected, interrupting a few scans with its warnings.

After some struggles extracting scan data from a series of XML files and allowing the on-access scanner to delete most of the infected test set, results were obtained. The results proved as excellent as those achieved by other products using the *Kaspersky* engine.

With detection almost impeccable and false alarms completely absent, *Redstone* qualifies for its first VB100 award.

Sophos Anti-Virus 7.0.6

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	99.80%
Polymorphic	100.00%	**False positives**	0

The entire *Sophos* product line has a resolutely corporate focus, and thus the offering for this test seems identical to those that have appeared in previous comparatives. With the usability never too taxing, the installation and configuration of the product slid by without any trouble.

Testing proved just as simple a process, although the progress bar proved as errant as ever (which proved to be a common issue in this test in cases where an attempt was made to estimate the remaining scanning time), and the logging seemed rather strangely organised and confusing.

The deep configuration available did not extend to scanning archives beyond five levels deep, but most types were covered, and scanning speeds – excellent with the default settings – were fairly good.

Detection rates were splendid, and although the switching on of a wider range of suspicious detection flagged up a number of unusually packed files in the clean set, alongside a handful of 'adware/PUA' and 'Hacktool' alerts, no full false positives arose and *Sophos* is able to claim another VB100 award after a couple of unlucky months.

Symantec Endpoint Protection 11.0.780.1109

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	100.00%
Polymorphic	100.00%	**False positives**	0

Symantec's corporate desktop product has undergone a considerable change recently, and still seems to be suffering a few teething problems.

Although the installation was impressively speedy, the automatic attempt at online updating took some time and effort to put a stop to (including a warning that it may take a few minutes to 'clean up'), followed by a reboot.

Logging of scan results also proved problematic, with attempts to open the logs via the interface causing some nasty freezes for the on-access data, and simply a blank page for on-demand data, despite several scans and several tens of thousands of items detected. The freezes were resolved by killing the process with the Task Manager, which brought up an increasing number of alert messages from *Symantec*'s anti-tamper system, informing me that attempts to shut it down had been 'blocked' – in one instance, after several dozen of these messages protection was in fact stopped and the interface restarted.

These minor issues, likely due to the generation of a log exceeding 150MB, did little to affect the results themselves however. Scan times were fairly good, with on-demand defaults delving three levels deep into most archives and more available. The on-access scanner seemed to offer only limited configuration but did identify disguised file types. Parsing the enormous log showed superb detection rates and a complete absence of false positives, and *Symantec* also qualifies for a VB100 award.

VirusBuster VirusBuster for Windows Servers 5.3 b.57

ItW	99.82%	**Worms & bots**	99.91%
ItW (o/a)	99.82%	**DOS**	99.77%
File infector	99.21%	**Macro**	100.00%
Polymorphic	85.91%	**False positives**	0

VirusBuster's server product again seems much the same as the home-user version, with the addition of an MMC-based console for some extra configuration. This included options which seemed to imply archives would be scanned

internally on access, but apparently only cover normal executables renamed as archives to conceal their intentions (which would be ignored in the default modes).

The interface itself is pleasant if a little fiddly when setting up scans, and suffers a tendency to linger a little over saving its logs, even those with minimal content. This did little to dent a good performance in terms of both speed and detection, with no false alarms and the W32/Virut samples missed by the other products using the same engine causing no difficulties here – presumably due to a slightly later version of the detection data. However, one remaining item, a W32/VB worm variant, was missed, and although we are advised that detection was added to the product a week or so after the submission deadline, the missed detection prevents *VirusBuster* from attaining a VB100 award this month.

Webroot SpySweeper AntiSpyware with AntiVirus Corporate Edition 3.50.3578

ItW	100.00%	**Worms & bots**	100.00%
ItW (o/a)	100.00%	**DOS**	100.00%
File infector	100.00%	**Macro**	99.93%
Polymorphic	100.00%	**False positives**	0

Last on the list of products comes *Webroot*'s *SpySweeper*. This is *SpySweeper*'s second visit to the *VB* test bench, having made its debut – and gained VB100 status – in the June 2007 *XP* review (see *VB*, June 2007, p.10). The corporate version submitted here was considerably different from the home-user edition submitted previously.

After a rather drawn out installation and startup process, the product offers a fairly comprehensive interface with some apparently well-populated configuration pages. Unfortunately, these are initially greyed out, as the client system submitted is designed to cede all control to a management server. Some changes to the registry allowed access to the settings (after providing a password) and testing continued.

Problems did not end there however, as the on-demand scanner seemed to provide no option to scan only a given folder and the entire system had to be scanned – no small job in this case. On returning after leaving the scan running overnight I found that the test sets had been covered pretty thoroughly, and they were then replaced before attempting the on-access tests. These were again hampered by the product's rather unusual implementation, with on-read scanning deactivated by default and only functioning rather flakily once enabled. This rendered any speed results gathered somewhat suspect, and only detection results were obtained by copying all test sets to the system across the network.

As far as can be judged by feeling alone, the protection did seem to slow the machine's response time down noticeably, especially during the five or so minutes after a reboot when the system tray icon is whirring and the interface unavailable (presumably doing some sort of boot-up checks.) After several attempts yielded a usable log of detection, results turned out to be pretty good – close to the high level expected of the *Sophos* engine used in the product – bar a few file types not scanned with these settings. Without false positives either, *Webroot* earns another VB100 award this month.

CONCLUSIONS

After the deluge of problems detecting a handful of nasty polymorphic viruses in the last round of testing, it was good to see far better coverage of the WildList this time. Most products seemed to have resolved their issues with these items, with a small handful of the latest worms causing the majority of difficulties this month.

False positives hit a cluster of other products, but few suffered any major issues with false alerting, most only flagging single files. With only a small number of packages added to the clean test set this month, this was to be expected. Many of the problems were with files that have been in the set for some time without causing any problems, which suggests that adjustments to heuristics are the main cause of the niggles.

The addition of the archive scanning test, intended as an adjunct to the speed test to indicate how speed times are affected by the depth of scanning, has also provided some information on the breadth of configuration available in products. Running a server-based test, we expected to draw in mostly enterprise-level products, which one would expect to offer considerably more flexibility than home-user offerings. Enterprise admins have far more complex and varying requirements than the simpler needs of the home user, with marked differences in network layout and system uses from company to company, widely varying company policies to comply with and so on. By limiting the choices offered to their users and admins, some products may risk limiting their usefulness in the corporate arena.

Technical details

Tests were run on identical machines with *AMD Athlon64 3800+* dual core processors, 1GB RAM, 40GB and 200 GB dual hard disks, DVD/CD-ROM and 3.5-inch floppy drive, all running *Microsoft Windows Server 2003 Enterprise Edition R2 SP2*.