



# virus

## BULLETIN

Fighting malware and spam

## VB100 COMPARATIVE REVIEW ON WINDOWS 2003 SERVER R2

### INTRODUCTION

We reached something of a milestone this month, as shortly before this comparative got under way we announced some major changes to the way in which the VB100 will operate. With the recent unveiling by The WildList Organization of the Extended WildList – a significant expansion of the range of malware covered by the list – it was clear that some decision would have to be made as to how to incorporate the new sample set into our testing, and it seemed like a good time to roll in some more updates which have been in the pipeline for some time. As of the next test, we will be allowing all products access to the Internet for the bulk of our testing. This will allow us to measure the effectiveness of the ‘cloud’ lookup systems that more and more products are including these days, while for those yet to move in this direction it will also show how well more traditional local updates are kept up to date.

This change will affect our certification programme, with the core components – the WildList sample sets and our false positive testing – being run multiple times during the test period, and products required to achieve the same high standards we have always demanded on a continuous basis. We will also be adding some new sample sets which should more closely reflect the vendors’ ability to keep up with the latest threats, and will be running our speed and performance measures in a more realistic environment; we hope to add some new measures to the selection we currently report. As our RAP test includes a retrospective component which cannot be properly measured without denying products access to their latest updates, this part of the comparative will remain unchanged.

While we had hoped to include the new Extended WildList as part of the requirements for this month’s certification testing, it quickly became clear that a little more time was required for the new process to settle in, so it was decided that the new set of samples would be included this month as

a trial only, with detection rates reported but not included as part of the certification requirements. As of the next test however, we will be requiring full coverage of the Extended list, making further demands on the products hoping to achieve certification.

### PLATFORM AND TEST SETS

With all this on the horizon, the current test is the last that will operate in the way in which the VB100 has been run more or less since its introduction in 1998 – at least as far as the certification component is concerned. The platform for this last test is the suitably traditional *Windows Server 2003* which has been with us for quite some time. The server-grade sibling of the evergreen *XP* was first released in April 2003, with the R2 edition used in this test released in late 2005. Having visited the platform most years since its release, preparation for the test was fairly straightforward. The installation process is simple and relatively speedy, even with the addition of service packs to bring it up to the current minimum state, and after adding our standard suite of handy tools, installing the drivers required for networking and other basic functions, and adjusting the look and feel to suit our tastes, images were taken for the tests without undue complications. We were pleased to find the platform remains as stable and responsive as ever, with its footprint on disk considerably smaller than its more complicated successors.

The product deadline was set for 24 August, and the test sets were built around this date. The RAP sets were compiled using samples first seen in the three weeks before and one week following the deadline, and the trojans set and the worms and bots set were both put together from items gathered in the month prior to that period. Little adjustment was made to the set of polymorphic viruses, and the clean sets saw the routine tidying up of older samples and expansion with a selection of new packages, focusing

on business-related software in deference to the platform chosen for this month. Final figures showed the clean set weighing in at just over half a million files, around 140GB, with the four weeks of the RAP sets and the worms and bots set measuring around 30,000 samples each. The trojans set was a little larger at just over 150,000 unique files.

The WildList set was the first area to be affected by the recent changes to the way in which the list is compiled: the legacy naming scheme has been put into retirement, replacing the names that aim to reflect those used by anti-malware solutions with less human-readable reference IDs for each sample. This meant some tweaks to the way the samples are processed, and all samples were re-validated regardless of whether they were new appearances on the list or long-time regulars. A handful of true viruses were spotted in the set, including the nasty W32/Virut family which has been a regular for several years, causing a number of upsets with its complex polymorphism, and as usual the latest strain was replicated in large numbers to ensure detection approaches were fully exercised.

The new Extended WildList was also put through our validation processes, the samples mostly proving to be fairly unexciting trojans, although a few items appeared likely to be flagged only as greyware by some vendors. Most interestingly, a handful of *Android* samples were included in the list, a reflection of the increased targeting of mobile platforms by malware creators. These samples presented some problems for our testing approach, as many standard *Windows* security solutions are not designed to deal with such items. Even where detection for such items was available, we anticipated that many products would not pick up the files with their default on-access settings – many products are limited to checking a standard set of *Windows* executable file extensions and the files were mainly present in install package archives or as .dex format executables.

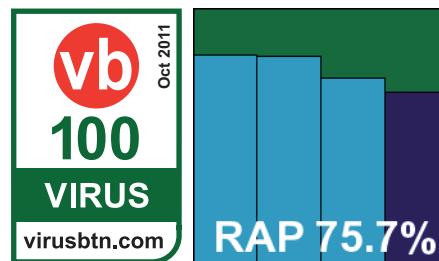
Product submission day brought no major surprises – a haul of 44 entries was around the anticipated number for a server test. A few major names were missing, and a handful of new products appeared for the first time, promising some interesting testing experiences. In a suitably sombre mood we embarked on the last comparative of its kind, preparing to bring an era to an appropriately solid end.

### Agnitum Outpost Security Suite Pro 7.5

Version 7.5.1 (3791.596.1681)

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	90.17%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.73%	<b>Trojans</b>	91.85%
<b>Extd. WL (o/a)</b>	99.27%	<b>False positives</b>	0

First up on this month's roster, *Agnitum's Outpost* product rarely misses a comparative these days and generally performs well,



although in recent tests we have noted some rather worrying lack of pace getting through our suite of tasks. The 95MB installer runs through a number of stages, mainly focusing on the firewall components which *Agnitum* specializes in, but gets through in reasonable time, completing with a reboot.

The interface is sturdy and businesslike without undue flashiness, providing a reasonable level of control for the anti-malware component, and for once tests ran through in decent time with no nasty surprises. Scanning speeds were not spectacular to start with but benefited greatly from some optimization in the warm runs, while on-access overheads were pretty heavy initially, again improving notably in the repeat measures. RAM usage was around average but CPU use was fairly high at busy times, with a pretty heavy impact on our set of standard tasks.

Detection rates were decent if again unspectacular, with solid coverage in most areas, declining fairly noticeably through the weeks of the RAP sets. In the new Extended WildList, a handful of items were not covered, although on demand most were in non-executable formats on this platform; there were a few more that were not blocked on access. The core certification areas were well handled though, and *Agnitum* earns another VB100 award.

The company has a solid record of late, with five passes in the last six tests, only the annual *Linux* test having been missed, and nine passes in the last two years. This month, all tests completed just about inside the 24-hour period planned for each product, with no crashes or other issues.

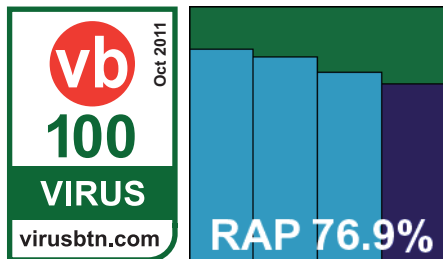
### AhnLab V3Net for Windows Server 7.0

Engine version 2011.08.23.93

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	86.79%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	92.46%
<b>Extd. WL</b>	99.36%	<b>Trojans</b>	87.67%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

*AhnLab's* product is another which routinely gives us a few headaches, usually with the logging system which rarely stands up to our heavy demands. The installer weighed in at 204MB, and after a few brief questions took some time to run through

its business, but no reboot was needed to complete the process. The interface is crisp and clean – a little confusing in places, but reasonably navigable – and provides a decent but not exhaustive level of fine-tuning.



Speeds were slightly below par on demand, and a little slower than average on access, with slightly high RAM use and a very high figure for CPU consumption at busy times – more than double the next highest measure this month. All this hard work paid off however, with our set of tasks zipped through very speedily.

Detection rates involved more hard work, with the unreliable logging system requiring us to split some of the tests into smaller chunks, and even then occasionally data could not be relied on and tests needed repeating. Scores were decent though, with reasonable levels in the main sets and a steady but not too steep decline through the RAP sets. A few items were missed in the new Extended WildList set, but on access at least these were all in non-standard formats not included in the usual list of scannable file types (mainly *Android* malware); somewhat oddly, several of these were spotted on demand, but a few others were ignored.

The clean set brought up the usual warnings on all OLE2 files containing macros, but no real false alarms, and with the WildList set properly handled a VB100 award is earned. *AhnLab's* recent history is a little unsteady, with three passes from four entries in the last six tests; six passes and three fails from nine attempts in the last two years. This month, thanks to the extra work required to coax usable logs out of the product, testing took a day and a half – a little more than planned but not excessively so, with no serious issues other than the less than robust logging system.

### ArcaBit ArcaVir 2011

Version 11.08.3203.1

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	68.83%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	N/A
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	N/A
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	4

*ArcaBit* continues to bravely try its hand in our tests, despite a lengthy run of bad luck. The current version was provided as a 150MB installer, including all required updates, and after

a fairly lengthy and silent pause at the beginning, the set-up process ran through a few rapid steps before another lengthy wait and finally completing. No reboot was needed.

The interface is fairly slick and attractive, although only basic controls are available, and in general it seemed fairly responsive (although trying to run one of the on-demand speed tests failed to produce the expected browser window, leaving the product completely frozen and requiring a reboot to get things back on track). Speed scores once gathered showed reasonable times on demand but quite heavy lag times on access, with low use of RAM and fairly high use of CPU cycles when busy, as well as a fairly high impact on the runtime of our suite of tasks.

Running the detection tests proved much more demanding, with scans repeatedly crashing out or freezing, and more freezes and crashes in the on-access tests. These were eventually completed after numerous retries, splitting the sets into smaller and smaller tasks. We found no specific samples that appeared to be causing the problems, implying that it was the sheer burden of our intensive tests that was bringing things to a crisis. On-demand jobs proved much more difficult, and several were abandoned after many days of hard work, with little to show for it.

On-access scores proved decent if unspectacular, and with the absence of any RAP scores or much else in the on-demand tests not much more can be said. The WildList and Extended WildList sets, being fairly small, were handled without difficulties, and both were covered excellently, with complete detection of both lists in both modes. In the clean sets however, a fairly large number of PDF files were flagged as potentially exploited, most of them sample documents included with *Adobe* products, and a handful of full false positives were also raised, including several items from major hardware brand *Belkin* and a component of a graphics package from *Corel*.

This was more than enough to deny *ArcaBit* VB100 certification once again, the vendor's record now showing no passes from four attempts in the last six tests; one pass and six fails from seven entries in the last two years. With the wealth of stability problems encountered, and the lengthy if futile efforts made to get around them, the product took up several of our test systems for well over a full working week before we finally admitted defeat.

### Avast Software avast! File Server Security

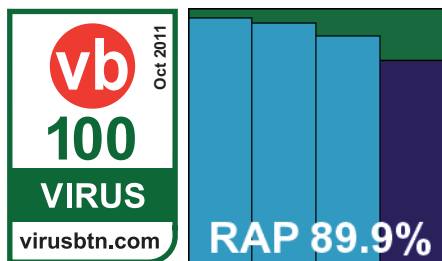
Version 6.0.1253

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.48%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.36%	<b>Trojans</b>	99.29%
<b>Extd. WL (o/a)</b>	99.27%	<b>False positives</b>	0

On-demand tests	WildList		Extended WildList		Worms & bots		Polymorphic viruses		Trojans		Clean Sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost	0	100.00%	3	99.73%	3879	90.17%	0	100.00%	13925	91.85%		
AhnLab V3Net	0	100.00%	7	99.36%	5211	86.79%	1704	92.46%	21062	87.67%		32
ArcaBit ArcaVir	0	100.00%	0	100.00%	12295	68.83%	NA	NA	NA	NA	4	11
Avast! Free	0	100.00%	7	99.36%	204	99.48%	0	100.00%	1216	99.29%		
Avertive VirusTect	0	100.00%	82	92.54%	4039	89.76%	0	100.00%	16498	90.34%		
AVG IS	0	100.00%	3	99.73%	382	99.03%	5	99.99%	3906	97.71%		3
Avira AntiVir	0	100.00%	1	99.91%	165	99.58%	0	100.00%	1821	98.93%		
BitDefender Security	0	100.00%	0	100.00%	149	99.62%	0	100.00%	1215	99.29%		103
BullGuard Antivirus	0	100.00%	0	100.00%	152	99.61%	0	100.00%	1317	99.23%		
Central Command Vexira	0	100.00%	6	99.45%	4298	89.10%	0	100.00%	15812	90.75%		
Clearsight Antivirus	0	100.00%	82	92.54%	4039	89.76%	0	100.00%	16498	90.34%		
CommTouch Command	0	100.00%	5	99.55%	10071	74.47%	0	100.00%	33451	80.42%	1	4
Comodo Antivirus	1	99.79%	8	99.27%	4147	89.49%	220	97.64%	43792	74.37%		
Comodo IS	1	99.79%	8	99.27%	4147	89.49%	220	97.64%	43792	74.37%		
Coranti Cora	0	100.00%	2	99.82%	7361	81.34%	0	100.00%	29655	82.64%		
Defenx Security Suite	0	100.00%	1	99.91%	3806	90.35%	0	100.00%	12904	92.45%		
Digital Defender	0	100.00%	82	92.54%	4039	89.76%	0	100.00%	16498	90.34%		
eEye Blink Server	0	100.00%	5	99.55%	3964	89.95%	4	99.98%	13466	92.12%		4
Emsisoft Anti-Malware	0	100.00%	2	99.82%	593	98.50%	36	99.81%	1497	99.12%	2	
eScan IS	0	100.00%	0	100.00%	151	99.62%	0	100.00%	1330	99.22%		
ESET NOD32	0	100.00%	0	100.00%	1271	96.78%	0	100.00%	5561	96.75%		22
ESTsoft ALYac	0	100.00%	3	99.73%	245	99.38%	0	100.00%	3545	97.93%		34

(Please see text for full product names.)

Moving onto a product with a rather more reliable record in our tests, Avast has an extremely solid run of test success



behind it, and with the arrival of the vendor’s latest and shiniest server version for the first time on the test bench we expected great things.

The 76MB installer runs through fairly quickly, looking slick and glossy, and needs no reboot to get most components working, although the sandboxing system is not fully active until after a restart.

Initial testing zipped through in good time, with some good speeds, medium RAM use and barely any effect on the speed of our set of tasks. However, CPU use was a little higher than average during busy periods. The on-demand detection tests blasted through with their usual rock-solid, no-prisoners attitude, and we moved onto the on-access tests expecting more of the same. In initial runs, however, we were surprised to see no sign of activity at all. Checking the settings, we observed that although the main homepage of the interface stated that protection was active, the page for the ‘Shield’ system reported its status as ‘Unknown’. Trying to restart things brought up an error claiming the shield was ‘unreachable’. Rebooting and reinstalling on a fresh system failed to resolve the issue, but a final reinstall, with a full licence key applied rather than the trial, got things moving at last. It seems there are a few bugs yet to be ironed out in this fairly new product.

On-demand tests contd.	WildList		Extended WildList		Worms & bots		Polymorphic viruses		Trojans		Clean Sets	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Fortinet FortiClient	0	100.00%	0	100.00%	1577	96.00%	0	100.00%	4567	97.33%		
Frisk F-PROT	0	100.00%	4	99.64%	10314	73.85%	0	100.00%	34583	79.76%		2
F-Secure Anti-Virus	0	100.00%	6	99.45%	769	98.05%	0	100.00%	3838	97.75%		
G Data AntiVirus	0	100.00%	0	100.00%	11	99.97%	0	100.00%	126	99.93%		
GFI VIPRE Antivirus	0	100.00%	0	100.00%	174	99.56%	20	99.79%	1157	99.32%		
Hauri ViRobot Server	1	99.79%	3	99.73%	537	98.64%	4460	92.99%	6715	96.07%	1	2
Iolo System Shield	1	99.79%	48	95.63%	12208	69.05%	634	99.05%	38826	77.28%		
Kaspersky ES	0	100.00%	0	100.00%	1347	96.58%	0	100.00%	7090	95.85%		
Lightspeed TTC	87	81.95%	381	65.33%	16704	57.65%	811	94.86%	60183	64.78%	60	
Lumension EMSS	0	100.00%	2	99.82%	3881	90.16%	4	99.98%	11395	93.33%		4
Microsoft Forefront	0	100.00%	0	100.00%	1544	96.09%	0	100.00%	12992	92.40%		2
Norman EP	0	100.00%	9	99.18%	3825	90.30%	4	99.98%	11250	93.42%		2
Preventon Antivirus	0	100.00%	82	92.54%	4039	89.76%	0	100.00%	16498	90.34%		
Quick Heal	0	100.00%	6	99.45%	3621	90.82%	0	100.00%	17026	90.04%		
Returnil System Safe	0	100.00%	0	100.00%	10037	74.55%	0	100.00%	31307	81.68%	2	2
Rising IS	0	100.00%	7	99.36%	NA	NA	NA	NA	NA	NA	6	
Sophos ESC	0	100.00%	0	100.00%	8029	79.64%	0	100.00%	31095	81.80%		5
SPAMfighter VIRUSfighter	0	100.00%	82	92.54%	4485	88.63%	0	100.00%	18819	88.99%		
TGSoft VirIT eXplorer	253	47.51%	757	31.12%	23589	40.19%	12006	68.48%	131072	23.29%	3	
Total Defense r12	0	100.00%	0	100.00%	8185	79.25%	4	99.96%	31064	81.82%		
UtilTool Server Antivirus	0	100.00%	82	92.54%	4039	89.76%	0	100.00%	16498	90.34%		
VirusBuster	0	100.00%	6	99.45%	4298	89.10%	0	100.00%	15812	90.75%		

(Please see text for full product names.)

Once the protection system was up and running properly, we re-ran the speed and performance measures but found the results barely changed. The on-access detection test powered through in record time, showing some superb detection rates. Similarly high scores were achieved throughout the on-demand tests, with some more excellent figures across the RAP weeks, declining only slightly into the proactive week. The Extended WildList set showed a handful of misses including several standard *Windows* executables, but the standard list was handled flawlessly, and with no false alarms in the clean sets *Avast* manages a splendid turnaround, achieving a solid pass having been on the verge of being dismissed as untestable.

The company's strong record remains intact, with every test since 2008 entered and passed. Even with the problems encountered and the multiple reinstalls, the product's

extreme speeds over the larger test sets meant that testing took up no more than the expected 24 hours of system time.

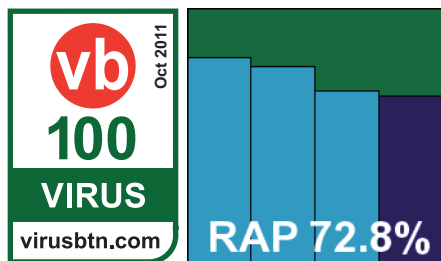
### Avertive VirusTect for Windows Servers

Version 1.1.69, Definitions version 14.0.179

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.76%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	90.34%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0

As has become a standard feature of our tests in the last few years, we saw a smattering of entries this month from near-identical products based on the *VirusBuster* engine via the *Preventon* SDK. *Avertive* is by now one of the more

familiar names on the ever-growing list. The 66MB install package ran through in just a handful of clicks, taking less than a minute to get set up with no reboot needed.



The interface hasn't changed much since our first sight of it: pleasantly clear and simple with a basic but usable range of controls. Stability has always been a strong point with this range of solutions, and most of the tests ran through without issues, although the product interface did seem to freeze up for a while after running our performance tests. Logging remains pesky, with the defaults set to dump old data after just a few MB has accumulated and a registry hack is required to change this. However, long experience has taught us to remember to make this change before running any tests for which full results are required.

Speed measures showed some fairly average throughputs and lags, with low use of resources and minimal impact on our set of standard activities. Scores were much as expected for the underlying engine – decent and respectable throughout with a steady drop through the RAP sets. The Extended WildList set brought the only real surprise, with a fair number of items not spotted in either mode, but the standard list was expertly handled, and with no false alarms in the clean sets a VB100 is comfortably earned by *Avertive*.

In the last year the product has achieved three passes from four attempts; three from five entries in the last two years. Testing took just a little over the scheduled 24 hours, with only a single minor issue observed during the run.

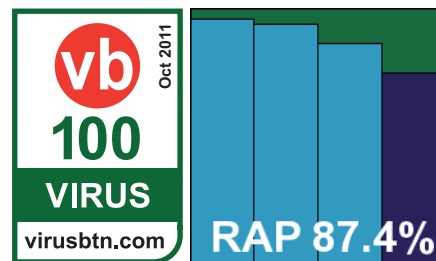
### AVG Internet Security Business Edition 2011

Version 10.0.1392

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.03%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.99%
<b>Extd. WL</b>	99.73%	<b>Trojans</b>	97.71%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

Another old-timer, *AVG's* business version is a pretty familiar sight on our test bench, looking fairly similar to the home-user variants anyway. The installer measured 169MB, and despite needing only a few clicks took some time to get itself set up, although no reboot was required. The interface is a little angular and tends towards fiddliness

in places, with some overlap of controls, but a good level of fine-tuning is available for those willing to dig it out.



Scanning speeds were perhaps a shade below average on first run, but blindingly quick on repeat attempts, with on-access overheads similarly improved after initial settling in. Performance tests showed medium use of memory and fairly high CPU use, but minimal slowdown in our set of tasks.

Running through the rest of the tests presented no problems, with everything running smoothly and stably throughout. Detection rates were very solid, with little missed anywhere, tapering off slightly in the later weeks of the RAP sets but still maintaining a pretty high standard even there. The core certification sets were handled impeccably, easily earning *AVG* another VB100 award, and even the Extended set was covered well, with only the handful of *Android* samples not alerted on.

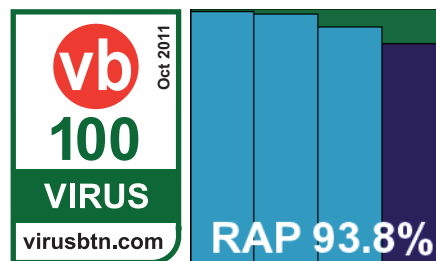
*AVG* thus recovers from a slight stumble last time, now showing five passes and a single fail from the last six tests; ten passes, one fail and one non-entry in the last two years. With no problems noted during testing, everything was completed within the single day allotted to the product.

### Avira AntiVir Server

Scan engine V8.02.06.40, Virus definition file V7.11.13.189

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.58%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.91%	<b>Trojans</b>	98.93%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

As usual, long-time regular *Avira* submitted a full server edition for our server test, with the complete product (including updates)



weighing in at under 70MB. The set-up process runs through a few stages, including the interesting step of

excluding items related to a selection of major services from scanning, but still gets through in splendid time with no reboot needed to complete.

The interface uses the MMC system, but is well designed, injecting a little colour for better visibility and pulling most of the comprehensive configuration controls out to more familiar window styles. Operation was thus fairly simple and generally stable, although we did note the scanner hanging at one point while scanning the local system drive. This was easily fixed however, and did not recur.

Speeds were no more than average and no sign of any optimization was seen on repeat runs. On-access overheads were a little heavier than many this month. Resource use was low on every count though, with very little slowdown in our set of tasks.

Detection rates were as stellar as ever, with very little missed across all our sets – even the later weeks of the RAP sets were demolished with some style. The Extended list was handled cleanly on access, with just a single item not detected on demand. Closer analysis of the logs showed that this item appeared with a line simply saying '[filepath] Warning – the file was ignored', where for everything else similar lines read '[filepath] DETECTION – [Detection ID] – Warning – the file was ignored', hinting that some kind of log writing error was behind this one.

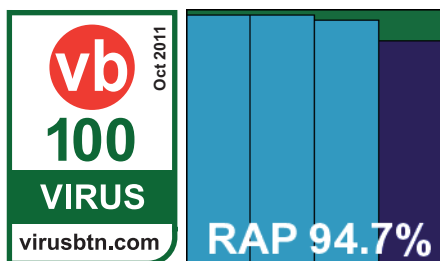
Meanwhile, the traditional WildList and clean sets were dealt with flawlessly, earning Avira another VB100 award for its cabinet. The vendor's test history shows a perfect record of passes in the last two years, 12 from 12 entries. With no major issues and excellent scan times in the infected sets all tests completed comfortably within our 24-hour window.

### BitDefender Security for File Servers

Version 3.5.17.8

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.62%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	99.29%
<b>Extd. WL (o/a)</b>	99.73%	<b>False positives</b>	0

Another fully fledged server edition, BitDefender's enterprise-ready solution came as a 182MB installer,



including all required data. The installation process takes some time, although interaction is not excessive and no reboot is needed. The GUI is again based on the MMC system, makes good use of colour and provides a clear and usable interface to a very full selection of fine-tuning options.

Testing ran through fairly smoothly, although on a few occasions larger scans of infected sets failed, but log data could be retrieved thanks to a new system of writing out to disk periodically rather than storing everything in memory. Speeds were pretty reasonable, with on-access overheads perhaps a little above average, and while RAM and CPU use were fairly low our set of tasks ran a little slower than usual.

Detection rates in the infected sets were extremely impressive, close to perfect in most areas and dipping only slightly below 90% in the proactive week of the RAP sets. Both the standard and Extended WildLists were impeccably handled with nothing missed on demand, and only the handful of odd Android samples in the Extended set ignored on access. The clean set showed no false alarms, although the resulting report was perhaps a little confused; having found no infections but a hundred or so password-protected files in our set, the final results screen warned that '6134439 files could not be cleaned'.

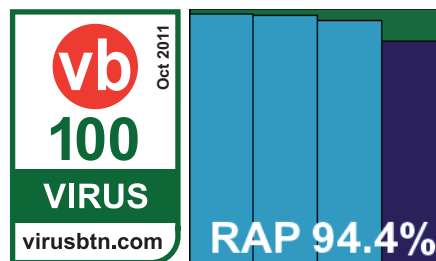
A VB100 award is easily earned despite this minor oddity, and BitDefender's record shows a full set of passes in the last six tests; ten passes, one fail and a single test skipped in the last two years. Despite a little extra interaction being required, testing powered through well within the expected time limit.

### BullGuard Antivirus 10

Version 10.0.190

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.61%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	99.23%
<b>Extd. WL (o/a)</b>	99.91%	<b>False positives</b>	0

Based on the BitDefender engine, BullGuard's solution is a much more consumer-focused suite solution, with its 157MB



installer needing only three clicks and blasting through in

On-access tests	WildList		Extended WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost	0	100.00%	8	99.27%	3975	89.92%	0	100.00%	16106	90.57%
AhnLab V3Net	0	100.00%	6	99.45%	3973	89.93%	138	99.78%	11782	93.10%
ArcaBit ArcaVir	0	100.00%	0	100.00%	12295	68.83%	731	93.63%	66645	61.00%
Avast! Free	0	100.00%	8	99.27%	252	99.36%	0	100.00%	1325	99.22%
Avertive VirusTect	0	100.00%	83	92.45%	4039	89.76%	0	100.00%	16498	90.34%
AVG IS	0	100.00%	6	99.45%	531	98.65%	5	99.99%	5367	96.86%
Avira AntiVir	0	100.00%	0	100.00%	187	99.53%	0	100.00%	1093	99.36%
BitDefender Security	0	100.00%	3	99.73%	147	99.63%	0	100.00%	1126	99.34%
BullGuard Antivirus	0	100.00%	1	99.91%	153	99.61%	0	100.00%	1654	99.03%
Central Command Vexira	0	100.00%	12	98.91%	3975	89.92%	0	100.00%	16219	90.51%
Clearsight Antivirus	0	100.00%	83	92.45%	4039	89.76%	0	100.00%	16498	90.34%
CommTouch Command	0	100.00%	9	99.18%	10393	73.65%	0	100.00%	35636	79.14%
Comodo Antivirus	1	99.79%	9	99.18%	4497	88.60%	220	97.64%	13728	91.97%
Comodo IS	1	99.79%	9	99.18%	4497	88.60%	220	97.64%	13728	91.97%
Coranti Cora	0	100.00%	6	99.45%	199	99.50%	0	100.00%	2084	98.78%
Defenx Security Suite	0	100.00%	8	99.27%	3975	89.92%	0	100.00%	16106	90.57%
Digital Defender	0	100.00%	83	92.45%	4039	89.76%	0	100.00%	16498	90.34%
eEye Blink Server	0	100.00%	169	84.62%	3990	89.88%	38	99.68%	11898	93.04%
Emsisoft Anti-Malware	0	100.00%	5	99.55%	NA	NA	NA	NA	NA	NA
eScan IS	0	100.00%	0	100.00%	207	99.48%	0	100.00%	3423	98.00%
ESET NOD32	0	100.00%	0	100.00%	1556	96.05%	0	100.00%	9608	94.38%
ESTsoft ALYac	0	100.00%	6	99.45%	247	99.37%	0	100.00%	3553	97.92%

(Please see text for full product names.)

impressive time, with no reboot necessary to complete. The interface is a little quirky but after some exploration proves pleasantly usable, providing a decent level of controls for its multiple components.

Testing ran through fairly smoothly and very rapidly, with some decent scan times speeding up massively in the warm runs, and on-access times similarly impressive after initial checks. Performance stats showed very low RAM use, CPU around average and impact on our set of jobs was fairly high.

Detection tests showed the expected excellent scores though, demolishing all our sets with ease. The core certification sets were dealt with impeccably, and just a single item in the Extended WildList was missed, on access only. A VB100 award is thus easily earned by *BullGuard*, whose test history shows four passes from four entries in the last six tests; seven from seven tries in the last two years.

With no issues noted and excellent speeds, all tests were out of the way after less than 24 hours of test machine time.

### Central Command Vexira Antivirus Server

Product version 7.1.75, Scan engine 5.3.0, Virus database 14.0.183

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.10%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.45%	<b>Trojans</b>	90.75%
<b>Extd. WL (o/a)</b>	98.91%	<b>False positives</b>	0

*Central Command* has built up a solid record in the last couple of years, after setting up a successful partnership with *VirusBuster*. *Central Command's* version of the product was provided as a 67MB installer plus a further

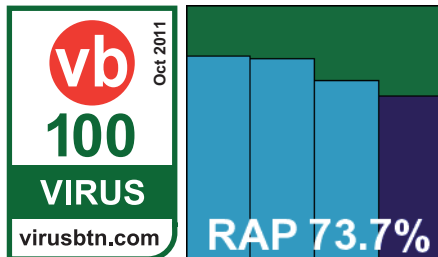


On-access tests contd.	WildList		Extended WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%	Missed	%
Fortinet FortiClient	0	100.00%	0	100.00%	1578	96.00%	0	100.00%	4567	97.33%
Frisk F-PROT	0	100.00%	6	99.45%	10454	73.50%	0	100.00%	36434	78.68%
F-Secure Anti-Virus	0	100.00%	6	99.45%	856	97.83%	0	100.00%	4187	97.55%
G Data AntiVirus	0	100.00%	0	100.00%	13	99.97%	0	100.00%	43	99.97%
GFI VIPRE Antivirus	0	100.00%	24	97.82%	633	98.40%	39	99.52%	6786	96.03%
Hauri ViRobot Server	1	99.79%	3	99.73%	588	98.51%	4447	93.00%	109851	35.71%
Iolo System Shield	0	100.00%	6	99.45%	10291	73.91%	0	100.00%	33449	80.42%
Kaspersky ES	0	100.00%	3	99.73%	2314	94.13%	0	100.00%	8640	94.94%
Lightspeed TTC	87	81.95%	381	65.33%	16704	57.65%	811	94.86%	60183	64.78%
Lumension EMSS	0	100.00%	2	99.82%	3881	90.16%	38	99.68%	11395	93.33%
Microsoft Forefront	0	100.00%	2	99.82%	1855	95.30%	0	100.00%	14777	91.35%
Norman EP	0	100.00%	2	99.82%	3980	89.91%	38	99.68%	11891	93.04%
Preventon Antivirus	0	100.00%	83	92.45%	4039	89.76%	0	100.00%	16498	90.34%
Quick Heal	0	100.00%	3	99.73%	10093	74.41%	0	100.00%	79513	53.46%
Returnil System Safe	0	100.00%	6	99.45%	10437	73.54%	0	100.00%	36349	78.73%
Rising IS	0	100.00%	6	99.45%	NA	NA	NA	NA	NA	NA
Sophos ESC	0	100.00%	1	99.91%	7762	80.32%	0	100.00%	28730	83.19%
SPAMfighter VIRUSfighter	0	100.00%	83	92.45%	4006	89.84%	0	100.00%	16409	90.40%
TGSoft VirIT eXplorer	254	47.30%	757	31.12%	23629	40.09%	23860	48.12%	128767	24.64%
Total Defense r12	0	100.00%	0	100.00%	8185	79.25%	4	99.96%	31064	81.82%
UtilTool Server Antivirus	0	100.00%	83	92.45%	4039	89.76%	0	100.00%	16498	90.34%
VirusBuster	0	100.00%	12	98.91%	3975	89.92%	0	100.00%	16219	90.51%

(Please see text for full product names.)

61MB of updates, and the set-up process was fairly complex with almost a dozen clicks required. It ran through fairly speedily though, requiring a reboot to complete.

Another MMC interface, this one is considerably less graceful than the others seen so far, with a clunky layout and less than easy navigation. A decent amount of control is available, but accessing and applying settings is far from fun.



Nevertheless we got through the tests without undue stress, with some decent scanning speeds and slightly high but not too intrusive overheads on access. RAM use was low and CPU use average, with impact on our set of tasks also not too heavy. Detection rates were reasonable if far from stellar, with decent coverage in most sets, dropping noticeably through the RAP sets. In the Extended WildList only the handful of non-standard file types were not covered on demand, while on access an additional half dozen executables were ignored. However, the traditional list was detected perfectly and with no false alarms in the clean sets *Central Command* wins another VB100 award.

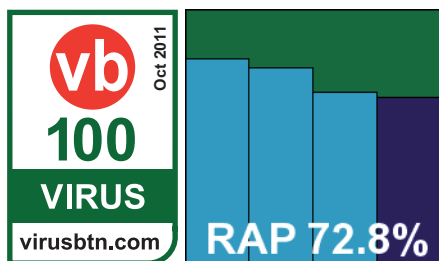
This makes ten awards from the last ten tests, a perfect record since the company's reappearance in the spring of 2009. With no issues emerging during testing and reasonable speeds, tests took just a little more than 24 hours to get through.

### Clearsight Antivirus

Version 1.1.69, Definitions version 14.0.179

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.76%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	90.34%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0

Another *Preventon!* *VirusBuster*-based product, *Clearsight's* 66MB installer ran through quickly with not too much interaction



demanding and no reboot required. The now over-familiar GUI remains simple to operate and provides a good basic set of controls. It generally ran well, although we did note a freeze during the scan of our clean set, requiring the scan to be restarted.

Speeds were pretty decent, with overheads a little higher than expected, including a spike hinting at another temporary freeze somewhere along the way. RAM and CPU use were around average, with not too much impact on our set of tasks.

Detection rates were much as expected – reasonable but not exceptional, covering most areas pretty well. Again a fair number of Extended WildList samples were missed, but the core certification sets were properly dealt with and *Clearsight* earns another VB100 award.

The vendor now has four passes from five attempts in the past year. A few minor slowdowns were noted, but nothing too serious, and testing took only a little longer than the one day scheduled for the product.

### Commtouch Command Anti-Malware

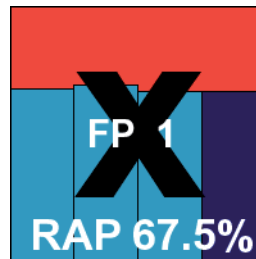
Product version 5.1.14, Engine version 5.3.5, Dat file ID 201108241005

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	74.47%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.55%	<b>Trojans</b>	80.42%
<b>Extd. WL (o/a)</b>	99.18%	<b>False positives</b>	1

*Commtouch* provided its current product as a tiny 12MB installer, with definitions arriving separately as a 28MB archive bundle. Installation started with a brief silent pause,

but then tripped through in just a few clicks with no need to restart. The interface remains minimalist and basic, but provides a usable level of controls and is generally simple to operate.

We noted no issues during testing, with scanning speeds a little below average and on-access overheads decidedly high. RAM use was low, but at busy times CPU use went through the roof, and the time taken to complete our set of activities more than doubled. Detection rates were distinctly unimpressive, with once again an odd hump in the middle of the RAP sets, other weeks staying remarkably stable. The Extended WildList contained a few undetected items, slightly more on access than on demand, as might be expected, but the main WildList set was well handled. In the clean sets, alongside a handful of alerts on items packed with Themida, a single item was flagged with a heuristic alert; on closer analysis, this appeared to be Welsh translations of *Linux* code, from a driver CD provided by major hardware manufacturer *Asus*. Apparently the code had sparked some emulation in the product engine, causing the heuristic rule to be tripped. This decidedly odd event was considered enough to deny *Commtouch* a VB100 award this month, despite a generally decent showing.



Such bad luck seems to be dogging the company of late, and it now has three passes and two fails from five entries in the last six tests; things seem to be looking up though, as the two-year picture shows four passes and four fails from eight attempts. With no stability problems, some slightly slow scanning speeds meant the full set of tests took about a day and a half to complete.

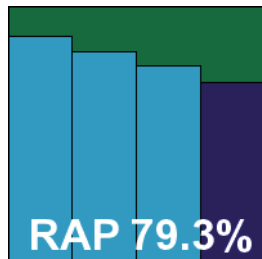
### Comodo Antivirus

Product version 5.4.191918.1356, Virus signature database version 9868

<b>ItW</b>	99.79%	<b>Worms &amp; bots</b>	89.49%
<b>ItW (o/a)</b>	99.79%	<b>Polymorphic</b>	97.64%
<b>Extd. WL</b>	99.27%	<b>Trojans</b>	74.37%
<b>Extd. WL (o/a)</b>	99.18%	<b>False positives</b>	0

Having put us through an epic waiting game in the last test, *Comodo* once again entered a brace of near-identical products, the first nominally being a plain anti-virus solution but still offering some advanced extras. The installation process was run online on the deadline day as no facility to provide offline updates was available; the 60MB installer ran fairly quickly, requiring a reboot,

then drew down around 120MB of additional update data. The GUI is quite a looker: angular but elegant, with a warm grey and red colour scheme. A good range of controls are available, with some common items that were noticed as missing from the product in recent tests having been added to this latest version.



Running through the initial tasks proved simple, with scanning speeds pretty good apart from over archives (which are scanned to some depth by default), while the on-access overheads were a little above average, the exception again being archives which, quite sensibly, are not touched in this mode. RAM use was low and CPU use above average, but our set of activities ran through very quickly indeed.

Moving onto the infected sets, scans once again took enormous amounts of time to complete. Whereas in the past this presented more of an annoyance than a problem, this time we also saw scans completing but failing to produce any results, claiming the system had run out of memory (our test machines have a mere 4GB available, but this should be ample for a consumer-grade solution). On-access detection tests were similarly slow. After many days we eventually gathered a full set of data, showing the expected reasonable scores in most areas, with a steady decline through the RAP sets. The Extended WildList was handled decently too, with just a handful of items not detected, and with the clean sets handled without problems for a change, all looked good for Comodo. In the WildList, however, a single item was missed in both modes, and a VB100 award remains just out of reach this month.

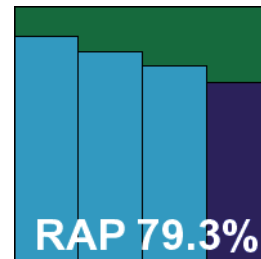
This plain anti-virus version has entered three times in the last year, four times in total, and has yet to record a pass. With the extreme length of time required to get through our test sets, and the re-runs required after logging failed, the product took up one of our test machines for more than 14 full days.

### Comodo Internet Security PREMIUM

Product version 5.4.191918.1356, Virus signature database version 9868

<b>ItW</b>	99.79%	<b>Worms &amp; bots</b>	89.49%
<b>ItW (o/a)</b>	99.79%	<b>Polymorphic</b>	97.64%
<b>Extd. WL</b>	99.27%	<b>Trojans</b>	74.37%
<b>Extd. WL (o/a)</b>	99.18%	<b>False positives</b>	0

The full suite version of Comodo's product installs from the same package as the plain anti-virus, with some extra options checked to include the firewall component and 'Geek Buddy' support system. This adds a few steps and a little more time to the installation process, and again a reboot and download of 120MB of updates is required. The interface is very similar, with just the extra module for the firewall controls, and again operation proved reasonably smooth and simple.



Scanning speeds and overheads were fairly similar to the plain product, scans slightly faster and overheads generally a little lighter, with RAM use and impact on our set of tasks again very low, CPU use a little above average. The infected tests took an age once more, and again we noted some issues with the logging and memory use. Detection scores were identical: respectable in most areas with some steps down through the RAP sets, and again the certification sets were mostly well handled with just a single item in the WildList set letting the side down, so no VB100 award could be granted.

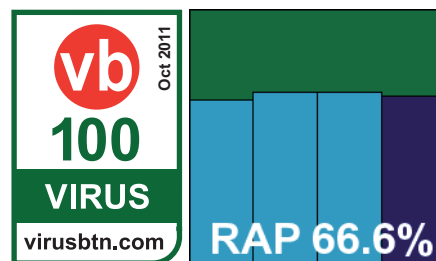
This suite version has notched up one pass in the past, and now shows one pass from four attempts in the last year; one success from five entries in total.

### Coranti Cora Antivirus

Product version 2.003.00005, Definitions database v.10818

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	81.34%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.82%	<b>Trojans</b>	82.64%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

Coranti has made several appearances of late with its remarkable multi-engine product, but this month's submission, we were informed,



was an entirely separate product provided by the company's Ukrainian spin-off. On the surface, however, it looked like business as usual, with a compact 12MB installer running through very quickly (offering English, Russian

On-demand throughput (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	34.01	2.57	2906.94	2.57	18.04	821.02	18.04	7.94	223.91	16.26	9.41	135.25	9.41
AhnLab V3Net	10.27	3.33	3.42	3.33	15.54	8.48	15.54	14.31	17.59	29.32	5.79	5.38	5.79
ArcaBit ArcaVir	16.35	8.21	8.50	8.21	20.44	20.79	20.44	11.13	28.47	22.81	13.36	13.70	13.36
Avast! Free	21.89	9.66	9.66	9.66	26.63	26.63	26.63	17.55	36.76	35.96	16.39	16.65	16.39
Avertive VirusTect	17.72	5.23	5.53	NA	19.09	20.02	19.09	15.41	35.19	31.58	6.68	7.07	10.61
AVG IS	71.87	4.55	2906.94	4.55	19.39	1642.04	19.39	9.50	615.76	19.47	4.77	216.40	4.77
Avira AntiVir	23.51	4.54	4.59	4.54	28.15	29.15	28.15	11.96	30.98	24.51	15.46	16.91	15.46
BitDefender Security	14.76	5.43	5.72	5.42	23.68	25.52	23.46	13.28	28.81	27.67	12.44	13.04	12.58
BullGuard Antivirus	15.68	12.11	2906.94	12.11	36.76	4926.11	36.76	16.25	2463.05	33.28	28.47	541.00	28.47
Central Command Vexira	18.05	11.91	12.11	4.03	17.66	18.04	17.98	19.55	41.40	29.15	18.98	19.32	15.24
Clearsight Antivirus	17.80	5.46	5.52	NA	19.47	20.11	19.47	15.61	34.69	31.99	10.93	11.63	10.93
CommTouch Command	18.05	4.69	7.49	4.69	18.24	18.45	18.24	10.45	21.23	21.42	11.51	11.63	11.51
Comodo Antivirus	11.69	2.23	2.24	2.23	19.86	20.19	19.86	24.29	50.78	49.76	20.04	20.42	20.04
Comodo IS	16.21	2.66	2.66	2.66	28.47	28.47	28.47	33.87	76.97	69.38	12.88	13.36	12.88
Coranti Cora	17.64	5.50	171.00	5.50	50.78	62.36	50.78	10.69	52.41	21.89	14.24	27.74	14.24
Defenx Security Suite	24.58	2.74	6.87	2.74	18.59	49.76	18.59	9.58	83.49	19.63	9.66	98.36	9.66
Digital Defender	17.64	5.13	5.17	5.13	15.11	15.69	15.11	10.50	29.32	21.51	12.02	12.88	12.02
eEye Blink Server	2.85	1.21	1.22	1.15	3.31	3.30	3.28	4.49	7.79	8.83	3.15	3.15	2.96
Emsisoft Anti-Malware	7.90	6.17	6.32	6.17	8.04	8.04	8.04	3.57	7.30	7.31	2.84	2.85	2.84
eScan IS	18.67	29.97	78.57	29.97	21.80	26.77	21.80	10.41	27.99	21.33	14.82	18.03	14.82
ESET NOD32	19.84	4.39	4.36	4.39	31.18	31.99	31.18	10.15	22.29	20.79	11.76	12.30	11.76
ESTsoft ALYac	22.67	116.28	322.99	2.94	17.91	447.83	17.91	8.94	307.88	18.31	8.87	90.17	8.87

\* System drive size measured before product installation

(Please see text for full product names.)

and Ukrainian as language options), then settling down to fetch 241MB of updates. This ran fairly quickly though, completing in less than 20 minutes, and the interface and user experience from there on was again similar to the mainline versions tested in the past. Simple, plain and unfussy, the GUI provides ample controls for the multiple engines and was generally responsive and stable throughout testing.

Speeds were surprisingly good, actually better than average in some areas and rarely much worse than the norm, while resource use and impact on our set of tasks were well within acceptable boundaries. Detection rates in the on-access tests were as excellent as might be expected, but when processing the on-demand logs the scores reported by

our processing tools were so unexpected that we re-ran all the tests, only to find exactly the same results. Comparing the scores with other products this month, and looking more closely at the logging, the problem immediately became clear: somehow, despite being labelled as active in the interface, some of the engines included in the product were not operational in the on-demand mode – usually the situation in which one would expect to see the most complete effort being made. Apparently this bug was quickly pinned down and fixed, but sadly for *Cora* it means the scores this month will be much lower than previous records set by its sister product.

Nevertheless, detection rates remained reasonable, and the core certification sets presented no issues, comfortably

On-demand throughput contd. (MB/s)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Fortinet FortiClient	16.49	9.00	9.26	9.00	11.05	11.51	11.05	20.04	40.71	41.05	10.71	10.50	10.71
Frisk F-PROT	22.54	10.89	10.97	10.89	15.49	15.59	15.49	12.52	26.48	25.66	16.91	17.45	16.91
F-Secure Anti-Virus	12.87	8.40	9.47	2.71	25.79	27.22	24.39	21.86	58.64	41.75	18.34	22.08	8.59
G Data AntiVirus	14.71	5.38	2906.94	5.38	24.03	2463.05	22.91	18.64	2463.05	38.19	13.20	541.00	13.20
GFI VIPRE Antivirus	13.00	3.15	3.16	3.15	17.16	17.53	17.16	3.35	6.88	6.86	1.52	1.41	1.52
Hauri ViRobot Server	6.35	126.39	484.49	6.35	32.62	447.83	32.62	32.94	259.27	67.48	15.03	72.13	15.03
Iolo System Shield	19.34	8.76	8.97	8.76	19.02	19.09	19.02	11.45	24.15	23.46	16.91	17.45	16.91
Kaspersky ES	37.72	2.97	968.98	2.97	12.25	234.58	12.25	9.32	80.76	19.09	7.31	27.05	7.31
Lightspeed TTC	13.70	2.67	2.43	2.67	18.04	17.85	18.04	3.67	15.11	7.51	7.31	7.41	7.31
Lumension EMSS	0.20	1.27	2.99	1.27	2.23	3.10	2.23	0.92	4.89	1.89	0.80	1.00	0.80
Microsoft Forefront	20.26	4.27	4.31	4.27	15.25	15.35	15.25	19.08	36.76	39.10	15.68	14.82	15.68
Norman EP	5.47	1.36	1.38	1.36	6.17	6.21	6.17	7.49	15.59	15.35	5.98	6.01	5.98
Preventon Antivirus	14.65	5.29	5.22	NA	16.70	17.22	16.64	12.02	26.48	24.63	13.04	13.70	13.04
Quick Heal	15.06	2.88	2.94	2.87	51.31	53.54	47.37	10.59	22.49	20.44	14.05	14.24	10.50
Returnil System Safe	16.01	4.72	4.70	4.72	13.31	13.53	13.31	4.74	9.85	9.72	9.75	9.75	9.75
Rising IS	13.18	4.85	322.99	4.85	6.25	6.30	6.25	9.43	25.26	19.32	10.02	12.02	10.02
Sophos ESC	15.06	1.61	1.62	1.61	20.44	20.79	20.44	18.79	40.71	38.49	14.82	15.03	14.82
SPAMfighter VIRUSfighter	16.93	5.47	5.05	NA	18.31	19.63	18.31	14.40	33.74	29.50	10.71	11.51	10.71
TGSoft VirIT eXplorer	13.80	181.68	181.68	NA	19.02	19.09	19.02	21.86	43.98	44.78	18.98	19.32	18.98
Total Defense r12	42.33	138.43	1453.47	3.63	33.74	1231.53	30.98	21.47	703.73	37.89	18.98	216.40	16.91
UtilTool Server Antivirus	15.00	5.40	5.44	NA	16.48	17.10	16.48	12.14	27.37	24.88	13.53	13.70	13.70
VirusBuster	13.85	11.67	11.82	4.01	15.54	15.94	15.30	14.66	34.45	25.93	15.46	22.08	12.44

\* System drive size measured before product installation

(Please see text for full product names.)

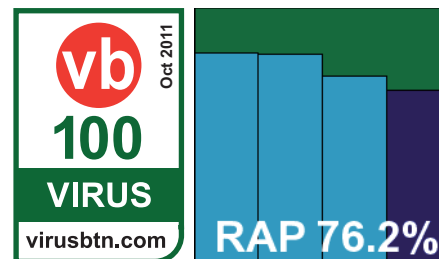
earning *Cora* a VB100 award at its first attempt. Even with the re-runs we performed in a surprised state, testing did not over-run by more than half a day, and the absence of the expected stratospheric detection rates were the only issue noted.

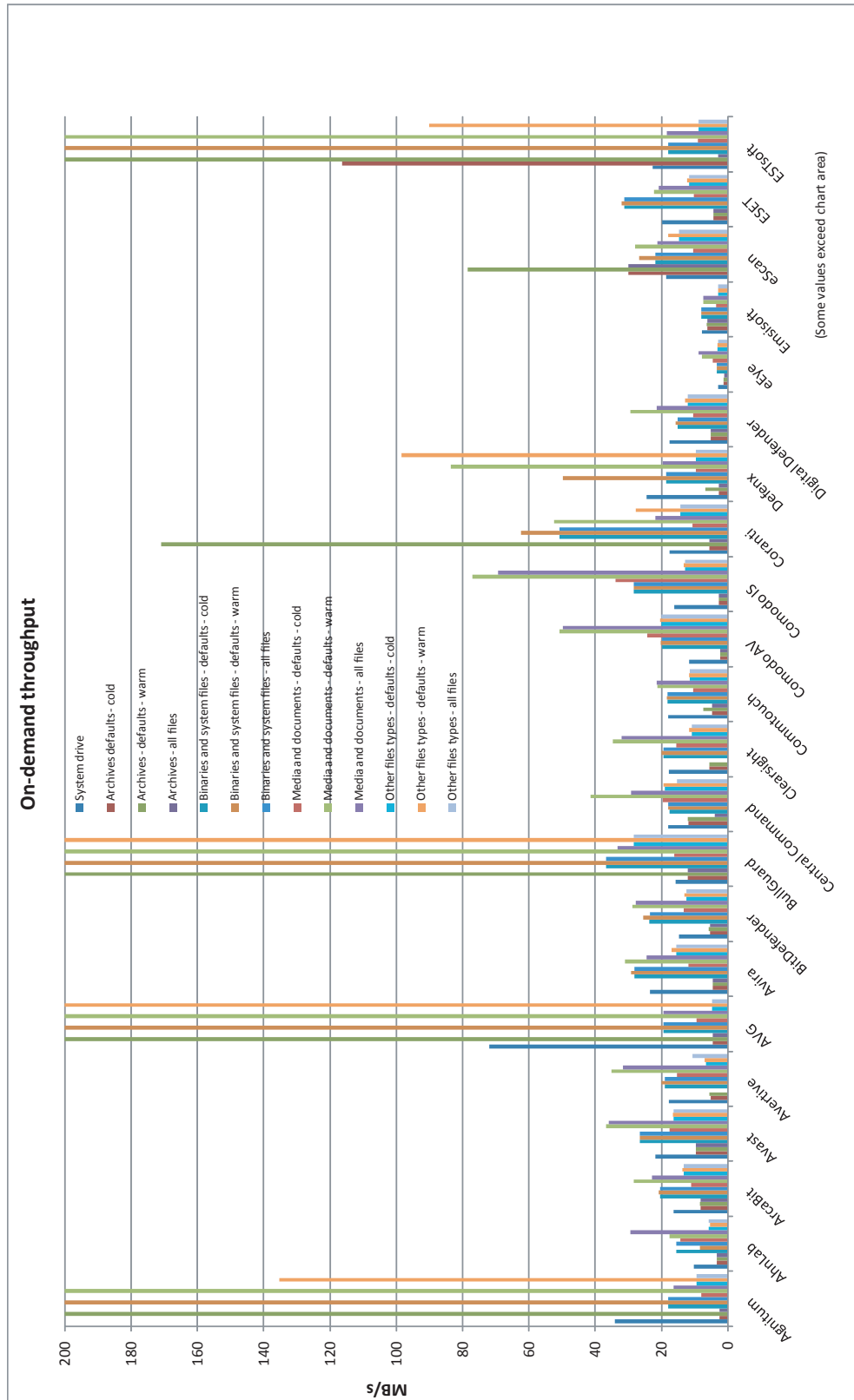
## Defenx Security Suite 2012

Version 3733.575.1669

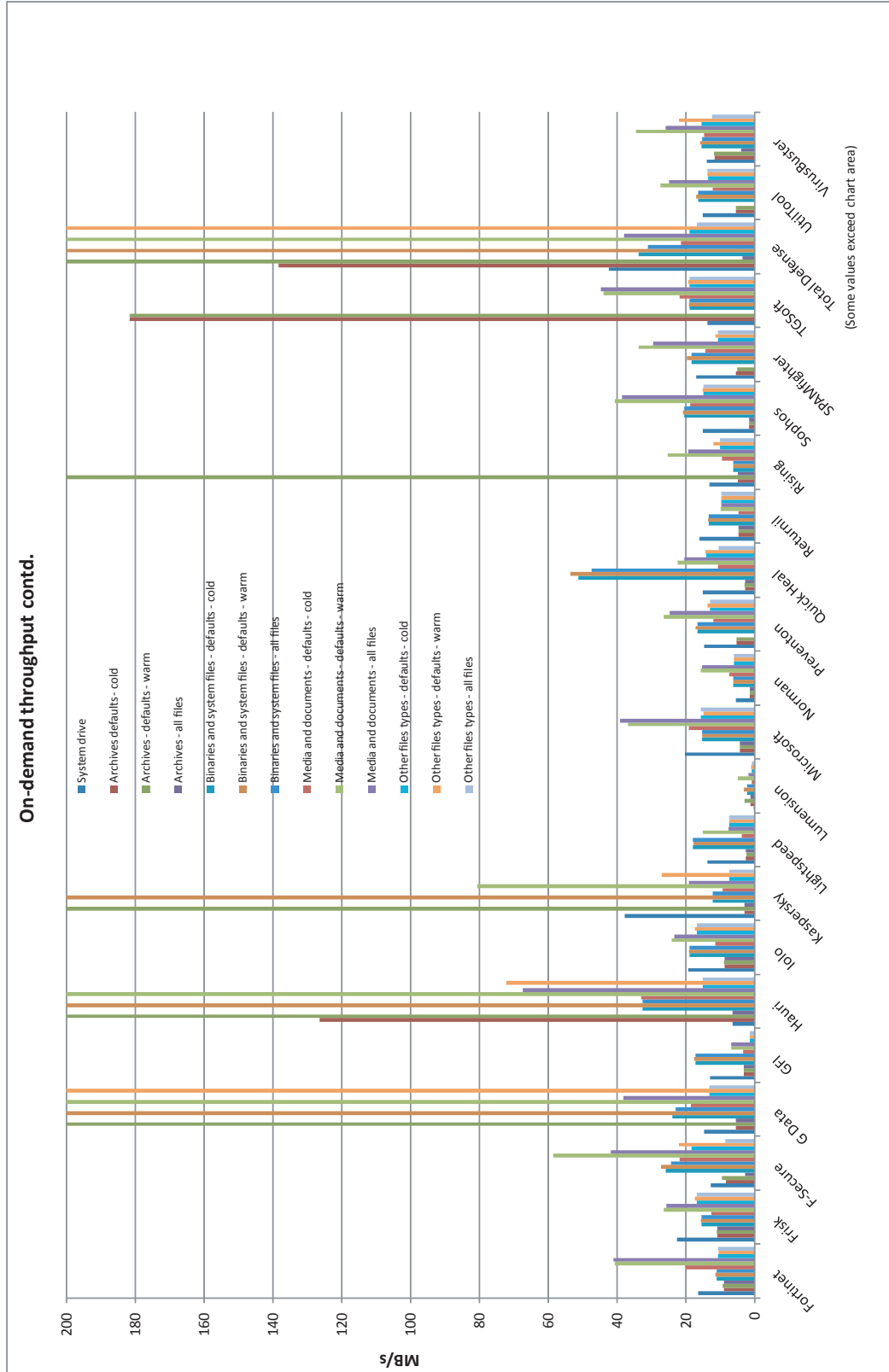
<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	90.35%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.91%	<b>Trojans</b>	92.45%
<b>Extd. WL (o/a)</b>	99.27%	<b>False positives</b>	0

Switzerland's *Defenx* has built itself up a nice history in our tests over the last year or so, and like its partner *Agnitum* has generally kept the lab team happy, apart from some rather disquieting slowness in the last couple of tests. Encouraged by *Agnitum's* performance this month, we hoped for a return to the solid and speedy tests of the past.





(Please see text for full product names.)



(Please see text for full product names.)

The installer was a fairly compact 96MB, and ran through in good time with not too much demanded of the user, finishing with a reboot and some initial set-up stages. As hoped, running through the tests proved painless, with reasonable speed measures and resource use showing slightly high consumption of CPU cycles and a noticeable effect on our set of tasks. Detection rates were much as expected – decent and respectable without challenging the leaders – and the core sets were managed comfortably without problems, earning *Defenx* another VB100 award.

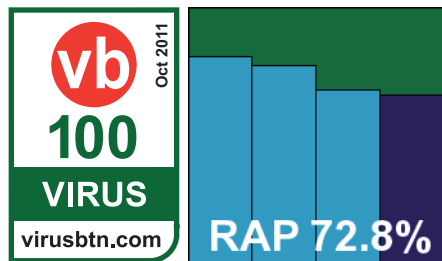
This gives the vendor five passes from five attempts in the last six tests, only the *Linux* test not entered, and nine passes from nine entries in total. Testing ran without issues and in good time, coming in just a few hours over the allotted 24.

### Digital Defender

Version 2.1.69, Definitions version 14.0.179

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.76%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	90.34%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0

Another *Preventon/ VirusBuster* offering, again with something of a history building up over recent months, *Digital Defender's*



product provided no surprises. The 66MB installer proved as fast and simple as expected, with no need to reboot, and the interface was clean and clear with a good basic set of controls. Testing ran through smoothly, with speeds a little on the slow side and overheads a little above average. Low use of RAM and low impact on our set of tasks was recorded, but fairly high CPU use at busy times.

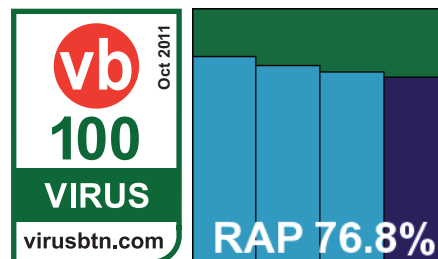
Detection rates were unremarkable but reliable, with most areas covered to a decent degree, and the core certification sets threw up no surprises, earning *Digital Defender* another VB100 award. That gives the vendor four passes from five attempts in the last six tests, its recent record showing great improvements after an earlier run of bad luck. The two-year figure shows five passes and four fails from nine entries. With no issues to report and reasonable speeds, testing completed in no more than a day and a half, keeping reasonably close to our schedule.

### eEye Digital Security Blink Server

Version 4.9.2

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.95%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.98%
<b>Extd. WL</b>	99.55%	<b>Trojans</b>	92.12%
<b>Extd. WL (o/a)</b>	84.62%	<b>False positives</b>	0

*Blink's* main speciality is vulnerability monitoring, but with the *Norman* engine included for malware detection it has been a regular



in our tests for some time. The submission this month was fairly large, with a 188MB installer supplemented by a 98MB update bundle, but the set-up process was fairly simple with a half-dozen clicks and a short wait while things were put in place, no reboot being required to complete. The interface is a sober grey for this server version, but little else seems different from the standard desktop client. Controls are reasonably accessible and provided to a respectable level of detail.

Testing took quite some time, with very slow speeds in the scan tests and pretty hefty slowdowns in the on-access measures, but our suite of tasks got through in decent time and RAM use was fairly normal, with fairly high CPU use at busy times. Detection rates were not bad, with decent coverage in most areas, dropping off steadily through the RAP weeks as expected. Despite a handful of items being missed in the Extended WildList, the main list was handled well, and the clean sets threw up a few suspicious alerts but no full false alarms. A VB100 award is duly earned by *eEye*.

The company now has four passes from five attempts in the last six tests, showing some recovery from a dark patch with four passes from nine entries in the last two years. With no problems other than the usual slow scan times – caused mainly by the in-depth emulation of the *Norman Sandbox* system – testing took a little more than two days to complete.

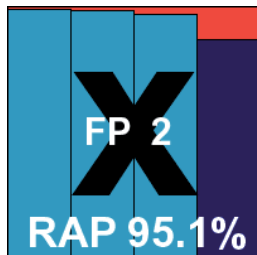
### Emsisoft Anti-Malware for Server

Version 5.1.0.16

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	98.50%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.81%
<b>Extd. WL</b>	99.82%	<b>Trojans</b>	99.12%
<b>Extd. WL (o/a)</b>	99.55%	<b>False positives</b>	2



Including the *Ikarus* scanning technology, the product formerly known as 'A-Squared' has become another OEM regular on our test bench. The current version came as a 120MB installer, with no further updates required, and installed in good time with no need to reboot. The interface is quirky and fairly limited as far as fine-tuning goes, but is fairly usable and generally responsive.



Scanning speeds were very slow, but overheads were not too bad, and RAM use was very low, with CPU use and impact on our suite of activities around average. On-demand detection tests ran well and showed some splendid scores, with excellent figures in the RAP sets, but on access things turned a little sour, the protection repeatedly falling over under the slightest pressure. Having nursed it through the smaller WildList sets, we wasted several days trying to coax some results out of it in the remaining sets, but eventually had to give up with time pressing.

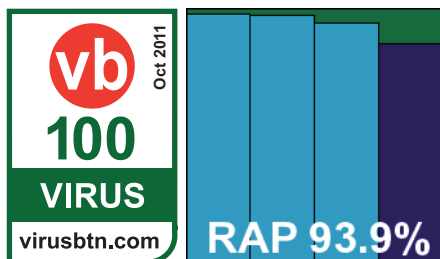
Scores in the WildList sets would have merited an award, with fairly small numbers missed in the Extended list too, but in the clean sets a couple of false alarms were raised on items from *Oracle*, denying certification to *Emsisoft* this month. A bit of a dry spell for the vendor, with only one pass from five tries in the last six tests; two passes from eight attempts overall. With some serious difficulties with the on-access scanner, and much work trying to get it to stay on for long enough to gather results, the product sat on one of our test systems for over a week.

### eScan Internet Security Suite

Version 11.0.1139.1048

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.62%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	99.22%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

The latest offering from *eScan* came as a 183MB installer including updates. Installation took some time to get through, with a fair number of clicks required



and several fairly lengthy pauses. On completion no reboot is needed, but the product launches straight into an initial scan. The interface is an odd combination of simple and flashy, with the plain angular top half jarring slightly with the slick, glossy icons at the bottom; the configuration controls under the hood sensibly stick to a more sober approach, providing an excellent level of control in a simple and easily navigated manner.

Running through the tests proved pleasingly unproblematic, with speed measures showing some good scan times and fairly light overheads. Resource use and impact on our set of tasks was also impressively low. Detection rates, as we predicted having seen those of other products including the *BitDefender* engine, were superb, all sets swept aside with barely a miss, RAP scores guaranteeing a strong position in the top corner of our chart. The WildList, including the Extended list, was covered perfectly, and with no issues in the clean sets a VB100 award is earned without breaking a sweat.

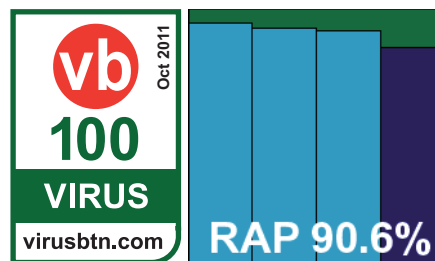
Our test history shows a decent record for *eScan* with five passes from the last six tests; nine passes and three fails in the last two years. With no problems and good speeds, all tests were completed within the allotted 24-hour period.

### ESET NOD32 Antivirus 4

Version 4.2.71.2, Virus signature database 6406

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	96.78%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	96.75%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

Still maintaining an epic streak of passes, *ESET* provided its latest product as a compact 49MB package, which installed with a simple process in good time. The interface remains attractive and pleasant to use, with good clarity in the main areas and a great level of fine-tuning under the covers. Operation was smooth and stable throughout testing, with no surprises or issues to report.



Speed measures showed decent scan times and reasonable overheads on access, with fairly low use of resources and fairly low impact on our suite of tasks. Detection rates were superb, with very solid coverage of all the sets, the reactive parts of the RAP sets showing only the slightest decline

File access lag time (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Agnitum Outpost	43.25	12.91	4.77	NA	50.39	9.91	50.39	107.34	31.06	107.34	99.94	6.72	99.94
AhnLab V3Net	36.65	15.44	14.21	15.44	32.28	31.67	32.28	64.22	63.38	64.22	50.41	49.58	50.41
ArcaBit ArcaVir	38.96	48.85	49.02	NA	49.42	50.84	49.42	76.60	67.94	76.60	46.14	43.24	46.14
Avast! Free	0.83	13.42	14.51	20.90	15.29	13.19	16.22	58.94	37.33	61.10	29.76	8.43	29.99
Avertive VirusTect	31.21	23.57	17.13	NA	47.81	39.88	46.01	10.67	2.77	56.79	44.90	15.47	74.64
AVG IS	4.87	1.37	0.98	4.79	36.83	1.18	1.40	56.64	7.66	15.15	100.80	22.29	51.02
Avira AntiVir	22.92	18.07	15.06	58.00	36.26	13.35	36.79	81.16	55.64	80.95	51.99	47.60	47.36
BitDefender Security	22.35	82.91	4.77	137.61	42.78	11.29	40.55	66.15	24.65	68.39	30.37	9.30	60.36
BullGuard Antivirus	18.15	97.74	22.47	NA	33.34	4.14	33.34	68.25	18.54	68.25	52.36	0.15	52.36
Central Command Vexira	30.14	5.99	5.05	6.81	58.22	39.56	40.57	71.58	56.45	69.30	68.39	63.07	76.38
Clearsight Antivirus	32.48	23.40	24.55	183.37	47.80	47.32	48.16	10.50	3.60	62.99	42.79	19.02	81.07
CommTouch Command	32.51	87.03	87.15	NA	50.79	50.97	51.61	140.10	139.41	141.03	70.74	69.81	91.33
Comodo Antivirus	46.92	5.62	3.19	NA	51.54	49.47	51.54	33.36	32.72	33.36	57.73	57.50	57.73
Comodo IS	43.96	3.78	1.38	NA	47.79	45.32	47.79	17.03	12.81	17.03	89.16	65.92	89.16
Coranti Cora	11.61	14.19	5.59	16.00	79.93	16.29	73.01	83.74	35.07	116.87	68.98	15.95	92.13
Defenx Security Suite	5.89	12.09	4.29	12.09	54.31	11.72	54.31	93.99	25.16	93.99	92.54	8.64	92.54
Digital Defender	30.82	36.01	29.92	NA	63.29	53.66	63.12	59.12	37.46	211.43	30.02	9.51	22.38
eEye Blink Server	60.54	6.11	6.87	NA	89.89	83.27	89.89	214.95	213.88	214.95	260.74	258.76	260.74
Emsisoft Anti-Malware	11.44	22.76	7.70	NA	62.71	3.79	62.71	73.66	16.03	73.66	1.79	0.96	1.79
eScan IS	20.65	13.35	5.16	NA	30.29	8.73	30.29	74.99	27.97	74.99	55.19	3.13	55.19
ESET NOD32	5.42	13.89	15.08	13.89	22.71	20.67	22.71	97.85	87.96	97.85	54.95	48.39	54.95
ESTsoft ALYac	10.46	0.30	2.28	NA	4.61	2.17	4.61	23.57	19.78	23.57	10.77	1.95	10.77

\* System drive size measured before product installation

(Please see text for full product names.)

with a slightly more pronounced drop into the proactive set, but remaining impressive even here. The Extended WildList was handled impeccably, as were the core certification sets, and ESET easily adds another VB100 pass to its monster collection – the company can boast entering and passing every test since mid-2003. With no problems and decent speeds, testing fitted easily into the allotted 24 hours.

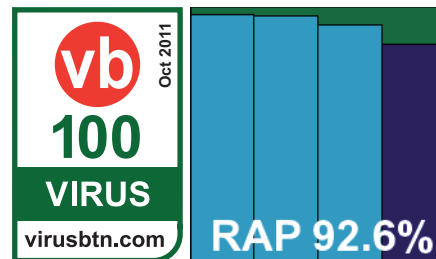
### ESTsoft ALYac Internet Security

Version 2.5.0.12

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.38%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%

<b>Extd. WL</b>	99.73%	<b>Trojans</b>	97.93%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

The first newcomer this month, the ESTsoft name may be familiar to some thanks to the unfortunate association of one of the company's other products with a mass hack attack in



File access lag time contd. (s/GB)	System drive*	Archive files			Binaries and system files			Media and documents			Other file types		
		Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files	Default (cold)	Default (warm)	All files
Fortinet FortiClient	24.01	101.10	2.31	NA	75.66	0.31	75.66	38.16	3.47	38.16	79.48	18.87	79.48
Frisk F-PROT	18.49	5.51	6.18	NA	51.14	51.78	51.14	35.64	34.31	35.64	30.50	29.54	30.50
F-Secure Anti-Virus	41.82	3.92	5.44	600.78	55.63	51.09	72.96	91.57	93.78	130.78	93.55	111.70	150.28
G Data AntiVirus	69.26	42.13	6.75	254.53	61.47	21.49	19.70	94.50	28.80	56.18	96.32	14.02	28.45
GFI VIPRE Antivirus	7.78	15.08	14.25	NA	49.44	21.77	49.44	553.27	59.83	553.27	492.69	39.97	492.69
Hauri ViRobot Server	16.61	0.36	2.06	NA	40.17	2.26	40.17	78.68	20.56	78.68	6.21	1.78	6.21
Iolo System Shield	32.08	86.62	88.10	86.62	50.34	50.87	50.34	137.23	140.17	137.23	69.98	69.72	69.98
Kaspersky ES	5.43	6.53	5.11	43.57	40.20	11.43	15.52	80.03	29.20	49.54	76.98	12.44	32.27
Lightspeed TTC	6.97	3.19	4.83	NA	36.83	8.47	36.83	45.52	26.90	45.52	16.75	1.81	16.75
Lumension EMSS	182.82	13.32	67.62	NA	269.85	181.82	269.85	429.52	341.29	429.52	299.93	381.89	299.93
Microsoft Forefront	2.68	4.23	2.65	NA	62.53	1.87	62.53	45.30	18.31	45.30	45.49	1.26	45.49
Norman EP	654.13	18.48	28.20	NA	179.87	183.05	179.87	286.11	292.86	286.11	369.00	412.45	369.00
Preventon Antivirus	41.04	29.14	22.36	NA	56.76	48.63	56.76	42.10	29.07	42.10	21.00	4.89	21.00
Quick Heal	17.35	28.67	29.38	NA	17.06	16.49	17.06	87.21	85.94	87.21	67.71	66.61	67.71
Returnil System Safe	22.45	25.13	26.78	NA	47.56	47.91	47.56	131.11	121.12	131.11	35.62	34.74	35.62
Rising IS	4.94	0.94	2.21	NA	1.90	2.04	1.90	21.49	18.83	21.49	6.08	2.71	6.08
Sophos ESC	23.87	7.42	8.80	590.61	43.40	43.27	47.65	37.51	32.07	43.23	36.40	34.60	44.29
SPAMfighter VIRUSfighter	36.40	22.63	23.82	111.68	47.55	46.81	47.24	10.79	3.79	59.95	45.37	18.95	75.84
TGSoft VirIT eXplorer	46.39	4.13	5.15	3.98	47.39	46.83	47.52	32.59	31.20	34.04	21.85	20.58	25.29
Total Defense r12	28.84	5.58	2.35	NA	29.15	11.42	29.15	48.37	27.75	48.37	42.61	13.13	42.61
UtilTool Server Antivirus	45.33	173.71	175.74	173.37	56.22	56.42	56.11	89.30	84.68	82.61	64.81	63.89	63.60
VirusBuster	30.14	5.99	5.05	6.81	58.22	39.56	40.57	71.58	56.45	69.30	68.39	63.07	76.38

\* System drive size measured before product installation

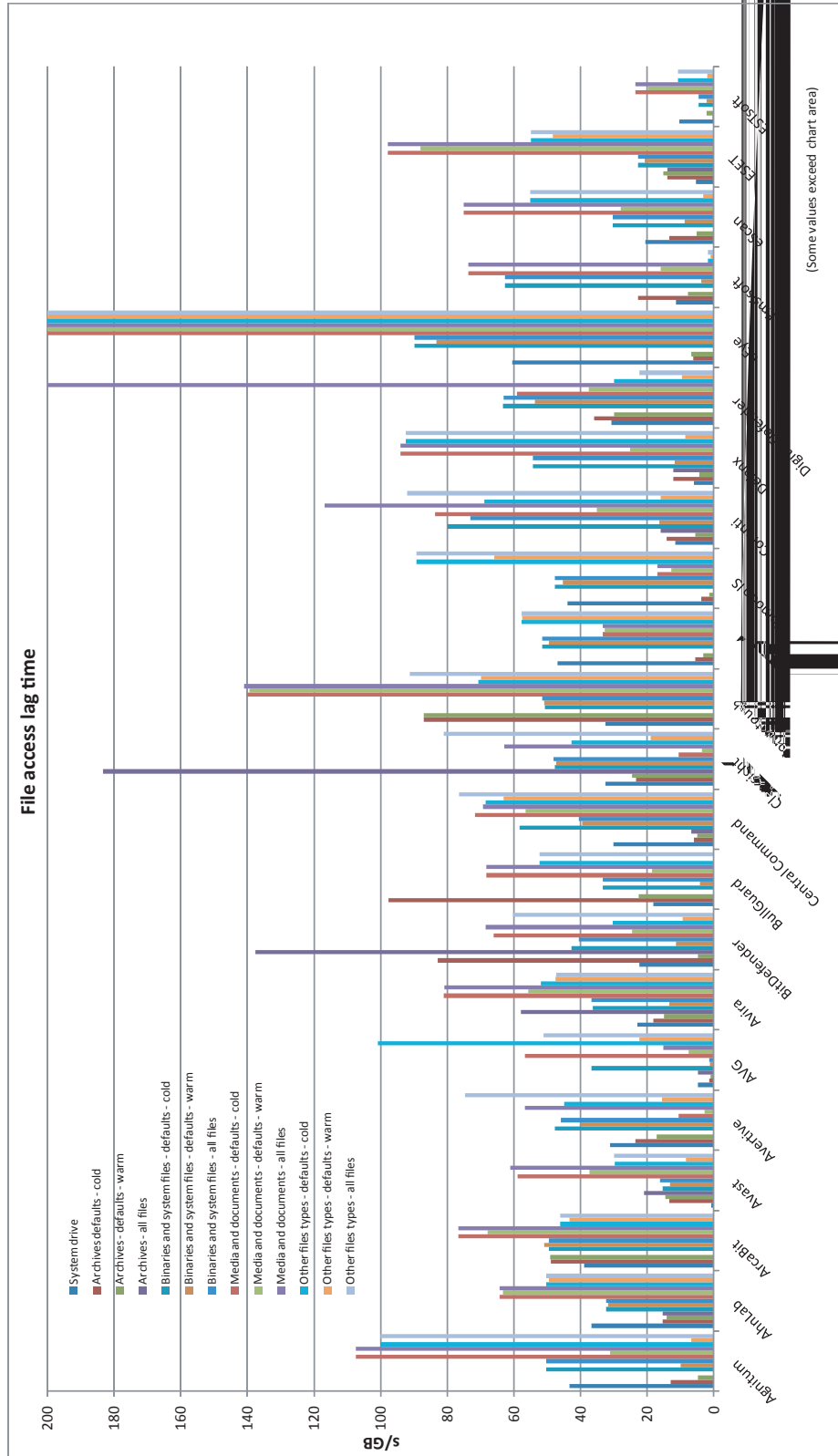
(Please see text for full product names.)

Korea a few months ago. The company's security product should be much sounder though, being based on the *BitDefender* engine which has already proved itself more than capable of handling our test sets this month.

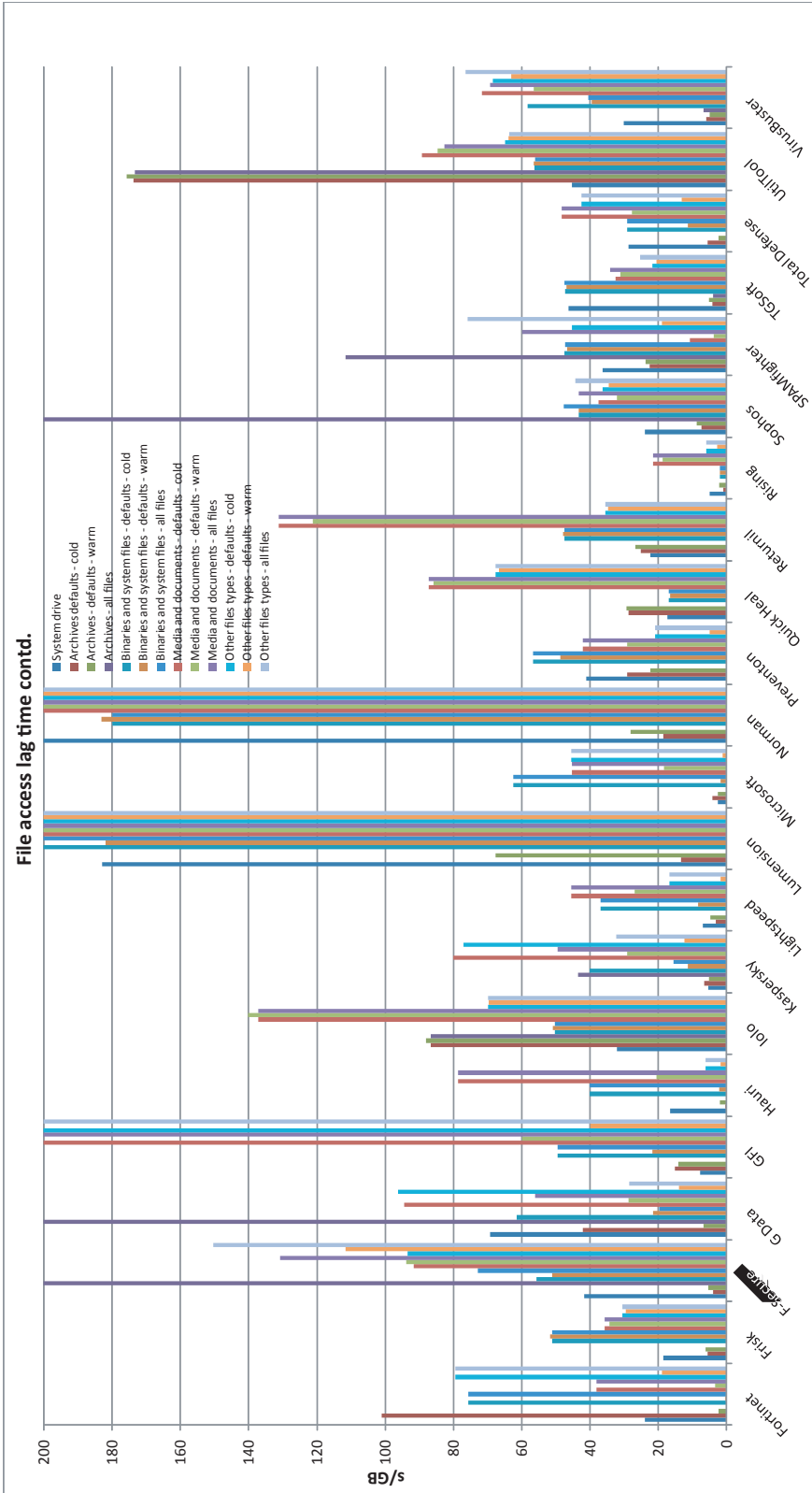
The product was sent in as a 153MB installer, which went through the usual set-up stages at a good rate, finishing with no need to reboot. The interface looks clean and simple; the 'AL' in the name is apparently Korean for 'egg', and a cartoony egg-shaped character adorns splash screens to lend the product a friendlier touch. Configuration areas are a bit plainer, providing a splendid degree of control, but the lab team felt a rather vague

sense of unease navigating things, probably due to the occasional infelicity of translation.

Running the tests proved smooth and problem-free, the product zipping through our sample sets with good speeds and low overheads. Resource consumption was comfortably below average and impact on our set of tasks not too intrusive. Detection rates were excellent as predicted, the scanner effortlessly blasting through the sets with barely a miss. With the certification requirements met without difficulty, *ESTsoft* earns its first VB100 award on its first attempt. No problems emerged, and testing completed well within the allotted time.



(Please see text for full product names.)



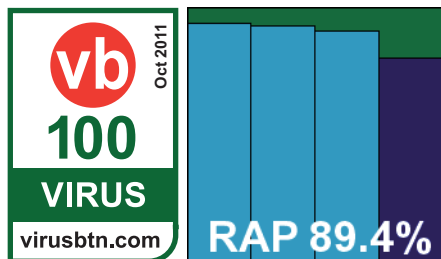
(Please see text for full product names.)

### Fortinet FortiClient

Version 4.1.3.143, AntiVirus engine 4.3.374, Virus signatures version 11.77

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	96.00%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	97.33%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

A rather more familiar name, *Fortinet* has shown some impressive improvements of late as *FortiClient* turns up its default



heuristics to great effect. The product remains compact at just 12MB, with definitions somewhat larger at 129MB. The installation process is rapid and straightforward, not taking long but needing a reboot to finish things off. The interface is plain and businesslike, providing all the controls required and with a simple and responsive user experience.

Testing was a pleasure, with no issues to report. Scanning speeds were not too fast, but on-access measures showed some good optimization after initial checking. Memory use was fairly low, CPU use fairly high but not outrageous, while impact on our set of tasks was perhaps a fraction above average. Detection rates were very solid though, with impressive scores everywhere but a fair-sized drop noticeable going into the final week of the RAP sets. The Extended WildList was fully covered, as was the more traditional list, and with no issues in the clean set a VB100 award is comfortably earned by *Fortinet*.

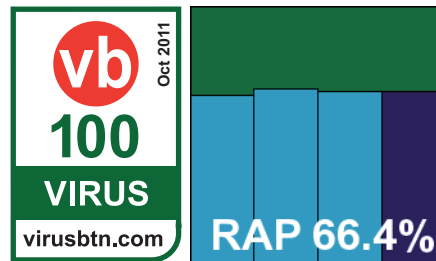
The long view shows four passes and a single fail from five attempts in the last six tests, the annual *Linux* test having been skipped, and the same pattern repeated in the previous year, adding up to eight passes from ten entries in the last two years. No problems were noted and testing ran through in good time, well within our scheduled slot.

### Frisk F-PROT Antivirus for Windows

Antivirus version number 6.0.9.5, Antivirus scanning engine version number 4.6.2

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	73.85%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.64%	<b>Trojans</b>	79.76%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

*Frisk's* product seems to have remained much the same for many years now, the 31MB installer and accompanying 27MB update



bundle being applied in a very familiar fashion, with only a few steps and a few seconds waiting before a reboot is demanded. On restart, the product seems rather slow to come online, refusing to open its GUI for almost a minute. Once it appears, the GUI is icily minimalist, with very few controls, and some of those that are provided are distinctly odd, but it remains pretty simple to operate and responded well during most of our tests.

Speed measures showed some reasonable rates, with on-access overheads a little above average; RAM use was fairly low, CPU use medium, and impact on our set of tasks barely noticeable.

On running the detection tests, scans died a few times (as we have come to expect) with the product's own error-reporting system sometimes allowing jobs to continue, while other times nothing short of a reboot was able to get things moving again. Detection rates were, as expected, fairly mediocre but reliable across the sets, with a handful of more obscure file types missed in the Extended WildList but no problems in the core certification sets, and *Frisk* earns another VB100 award without fuss.

The vendor's recent test history is good, with five of the last six tests passed; the longer term view is a little shakier, with eight passes and four fails in the last two years. The only issues observed were scan crashes when running over large infected sets (unlikely to affect real-world users). With some fairly slow speeds processing polymorphic samples, testing took close to two days to complete, but didn't knock us too far off schedule.

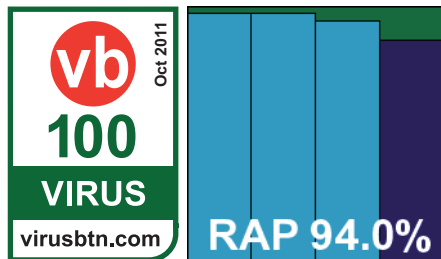
### F-Secure Anti-Virus for Windows Servers

Version 9.00 build 333, Anti-Virus 9.20 build 16040

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	98.05%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.45%	<b>Trojans</b>	97.75%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

Another cold climate vendor, *F-Secure* sticks to the icy white theme, the enterprise solution's 45MB installer (supplemented by 151MB of updates) running through quite

a few stages but needing no reboot to complete. The interface is cold and stark, running in a browser and suffering the usual



responsiveness and stability issues associated with such an approach. Configuration is fairly limited and at times inaccessible. On several occasions scans would not start, the interface getting itself tied into knots and needing a reboot to resolve matters.

We eventually got things moving along, with speed tests showing some reasonable scan times but fairly heavy overheads on access. RAM use was not high though, and CPU use not exceptional either, with a very low time for our suite of activities. Moving on to the detection tests, things ran through fine on access, but on-demand scans repeatedly dropped out without warning or explanation. Some in-depth diagnostics showed that specific files seemed to be tripping the scanner up. Trying to filter these files out over numerous scans proved too much work for our hard-pressed team, and in some areas we resorted to using the on-access scanner results only.

These showed some splendid scores, as expected from the results of other products that include the *BitDefender* technology, with most sets demolished and the Extended WildList only missing those odd items in non-executable formats. The main WildList and clean sets were handled impeccably, and a VB100 award is earned by *F-Secure*.

The last six tests show five passes from five entries; nine passes from nine attempts in the last two years, a solid record. With much work having gone into re-running crashed scans, the product took up at least four full days of test machine time this month. However, there were no issues that would be likely to emerge in everyday, real-world use.

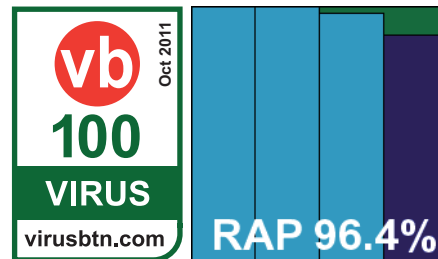
### G Data AntiVirus Administrator/Client

Program version 11.0.1.44, Virus signatures: Engine A: AVA 22.1766, Engine B: AVL 22.315

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.97%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	99.93%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

With both engines included in this product already having demonstrated strong performances this month, and the

product's multi-engine rivals either absent or hobbled by bugs, hopes were high for another stellar showing from *G Data*.



The enterprise product came in two parts, with an administration system provided as a 684MB installer and a client subsystem pushing 200MB. Setting up the admin component took quite some time and much interaction, with various dependencies resolved along the way, but the client part ran much more rapidly and with limited interaction. A reboot was required to get everything active.

With options available to offload responsibility for running scans and tweaking settings to the client, testing itself was fairly straightforward. The product's usual rapid warm scanning speeds kicked in during the speed tests, shooting off the top of the scale in the on-demand graph. On-access overheads as usual were reasonably light with the default settings, noticeably heavier with scan settings turned up high. RAM and CPU use were a touch above average, but our set of tasks were got through at a good speed.

Detection rates were as awesome as expected. The RAP sets were destroyed, even the proactive week pushing close to 90%, and the core certification sets were brushed aside in short order. *G Data* comfortably earns another VB100 award, the vendor's history showing four passes from five entries in the last six tests; eight from ten in the last two years. With no issues, solid dependability and decent speeds, all tests completed on schedule in less than a day.

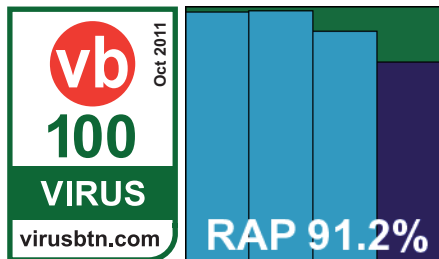
### GFI VIPRE Antivirus

VIPRE software version 4.0.4210, VIPRE engine version 3.9.2500.2, Definitions version 10257

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	99.56%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.79%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	99.32%
<b>Extd. WL (o/a)</b>	97.82%	<b>False positives</b>	0

Fully settling after the transition from *Sunbelt* to *GFI*, *VIPRE* has become a regular in our tests and seems to crop up ever more regularly as an OEM engine. The current version is a slimline 13MB main installer, with 72MB of updates also required, and the set-up process runs at average speed with a standard set of steps to follow. The interface is clear and bright without overdoing the styling, providing

a pretty basic set of controls – which are a little less than clear in places, but generally not too difficult to operate.



Scanning speeds were rather slow and on-access overheads a little on the high side, but use of RAM and impact on our set of tasks were both fairly low, with CPU use at busy times a little above average. Running the detection tests was as tiresome as ever, with logs stored in memory until the completion of scans which frequently died with a message stating that the scan ‘failed’ for no clear reason, leaving no usable data behind. On-access testing was also a little fiddly, with the product’s use of delayed checking meaning that our opener tool was regularly allowed access to a file for a few moments before the detection kicked in. This meant having to cross-reference the product’s rather unfriendly logs with our own data, and in the case of the on-demand tests re-running jobs many times with ever smaller subsets of our full set.

Eventually results were gathered however, and they showed some pretty impressive scores, dropping away fairly steeply in the proactive week of the RAP sets but remaining decent even there. The Extended WildList was covered flawlessly on demand but showed a few misses on access (possibly items considered merely grey as well as the handful of *Android* samples). The main WildList was handled well though, and with no false positives to report, a VB100 award is duly granted to *GFI* after great labours on our part.

The product’s test history shows five passes from five attempts in the last six tests; seven from eight attempts in the last two years. With the slow scanning and multiple re-runs required, not to mention the hard slog of turning logs into usable data, more than two full weeks of test lab time were taken up – many times the fair share we hoped each product would need.

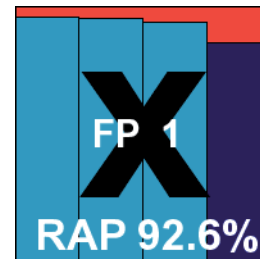
### Hauri ViRobot Server Protection 2011

Version 6.0.0, Engine version 2011-08-24.00(8965391)

<b>ItW</b>	99.79%	<b>Worms &amp; bots</b>	98.64%
<b>ItW (o/a)</b>	99.79%	<b>Polymorphic</b>	92.99%
<b>Extd. WL</b>	99.73%	<b>Trojans</b>	96.07%
<b>Extd. WL (o/a)</b>	99.73%	<b>False positives</b>	1

This is another product including the *BitDefender* engine, but one which routinely seems to have difficulties where

other products using the same technology do not. *Hauri’s ViRobot* is a sporadic entrant in our tests and last achieved a pass way back in 2003. The current version was provided as a 243MB installer including all updates, and ran through a number of stages, including the offer of a pre-install scan and some configuration options, taking quite some time to finish but needing no reboot. The interface is quite attractive – elegant and simple on the main screens but providing a lot of good controls under the covers. There is also some useful information provided, such as system resource use monitors presented in a pleasantly clear manner.



Running tests went pretty smoothly at first, with scanning speeds good to start with and super fast on repeat runs, on-access times likewise starting off pretty decent and becoming almost imperceptible once warmed up. Resource use was very low and our suite of activities ran through in splendid time. On-demand detection tests ran well, showing the excellent scores expected of the underlying engine in most areas, but the on-access tests proved a little more tricky, the protection system buckling under heavy pressure and apparently simply shutting down silently halfway through jobs. After several attempts we got a full set of results, tallying closely with the on-demand scores, with very impressive numbers in most areas.

Eagle-eyed readers will have noted the words ‘in most areas’ above, and the solid detection sadly did not extend quite broadly enough. Three samples were missed in the Extended WildList, all of them standard *Windows* malware, while a single item went undetected in the main WildList set. With a couple of false positives in the clean set too, *Hauri* does not quite reach the required standard for VB100 certification.

The vendor has had no luck from four attempts in the last year, and no entries before that for quite some time, but things seem to be gradually improving and we would expect to see a pass sometime soon, assuming we continue to see regular participation. The only problem encountered was the collapse of the real-time protection under heavy load – perhaps an unlikely situation in the real world, but it set our testing back somewhat and with the many re-runs required the product needed almost a week of lab time to get everything completed.

### Iolo System Shield

Version 4.2.4

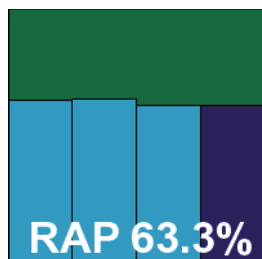
<b>ItW</b>	99.79%	<b>Worms &amp; bots</b>	69.05%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.05%



### Iolo System Shield contd.

<b>Extd. WL</b>	95.63%	<b>Trojans</b>	77.28%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	0

Another product insisting on installation and updating online on the deadline day, *Iolo* provided a tiny 450KB download tool which proceeded to fetch and install the main product. The installer brought down measured 48MB, and an option was provided to have it saved locally in case it was needed again in future. After the standard install steps, the set-up process was pretty fast, completing in less than a minute, then a reboot was requested before updates ran, again not taking too long to complete.



The interface has a fairly standard design and looks slick and professional, providing a surprisingly high degree of control under the hood for such a clearly consumer-focused solution – although there was still much absent which one would hope to see in a business product. The absence of a context-menu scan option, almost universal these days in desktop offerings, was rather a surprise.

Operation was fairly smooth and simple though, and speed tests ran through without issues, showing some reasonable scan times but fairly high overheads on access. RAM use was quite low but CPU activity was very high and our set of tasks seemed to take forever to complete. Moving on to the detection tests, we once again could find no option to simply log detections. Instead we opted to remove everything detected, but this seemed less than reliable. Logs are stored in an extremely gnarly binary format, and cannot be exported to file from the product interface, so we contacted the company asking for information on how to decrypt them – the fourth consecutive test where we have made such a plea for information. At least this time we got some response, claiming someone was looking into it, but when several weeks later we still had received no further help decrypting, we had to resort to some rough manual ripping apart of the data. Combining this with information on which files had been left on the system after several runs gave us some usable data which seemed close enough to the on-access scores and those of other products based on the same *Frisk* engine, that we assumed it to be reasonably accurate.

Detection rates were generally fairly mediocre, with respectable but not impressive rates in most areas; RAP scores place the product towards the lower end of the main cohort on our scatter graph. The Extended WildList

showed a handful of misses, and in the main list a single item seemed to go undetected in the on-demand mode only. Surprised by this, and assuming there had been some error in our brute-force log parsing, we repeatedly rechecked the sample, but found each time that no alert was produced and the file was left in place. Trying to copy the file elsewhere meant the on-access component kicked in and immediately alerted on it and removed it. Thus, despite an otherwise clear run through the clean sets, no VB100 award can be granted to *Iolo* this month.

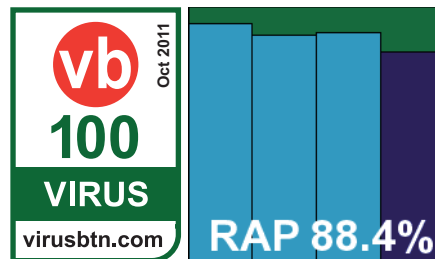
The product’s test history shows two passes from four attempts in the last six tests, with one additional entry in the last two years not adding to the tally of passes. Although testing ran in reasonable time, the apparent inconsistency of the on-demand scanner’s response to detections and the bizarre nature of the product’s logs, coupled with the company’s apparent inability to help out with this, meant that more than a week was taken up by this product.

### Kaspersky Endpoint Security 8 for Windows

Version 8.1.0.524

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	96.58%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	95.85%
<b>Extd. WL (o/a)</b>	99.73%	<b>False positives</b>	0

Back to a company with a long and pretty glorious history in our comparatives, but one which has also had some trouble describing the



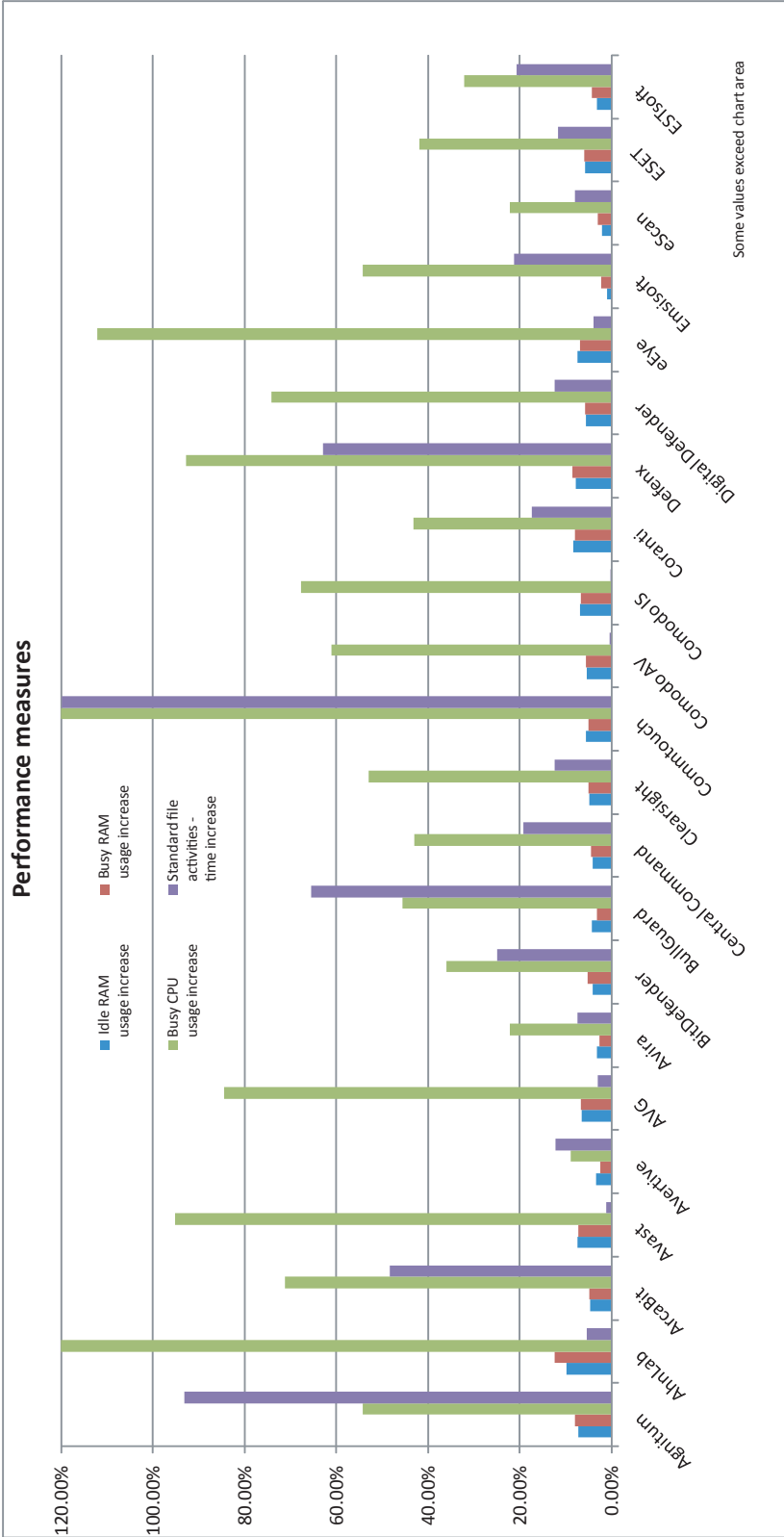
operation of its logging system in recent tests, *Kaspersky* provided its latest, shiniest enterprise solution this month, a late beta of the new corporate desktop product. The installer was a fair size at 127MB, with updates provided as a mirror of a complete update system supporting a range of products and thus also fairly large. The set-up process was a little slower than some this month, but still ran through in reasonable time with not too much demanded of the user, and needed no reboot to complete.

The interface is a considerable achievement: simple, elegant and highly efficient, providing the superb depth of fine-tuning we expect from *Kaspersky* without sacrificing usability. Some areas seem familiar from related products,

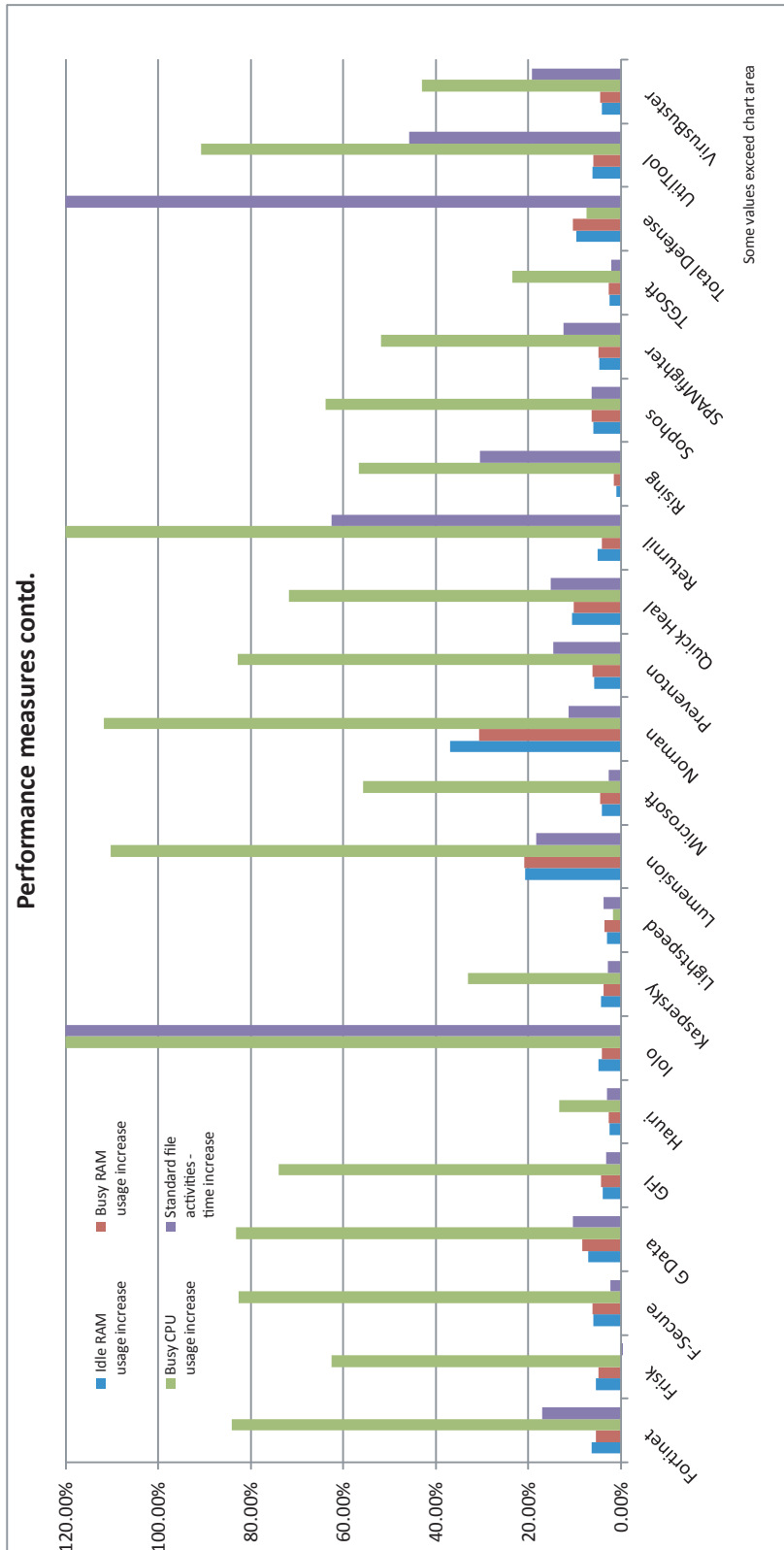
<b>Performance measures</b>	Idle RAM - usage increase	Busy RAM - usage increase	Busy CPU - usage increase	Standard file activities - time increase
Agnitum	7.24%	8.01%	54.28%	93.19%
AhnLab	9.84%	12.48%	330.62%	5.50%
ArcaBit	4.77%	4.88%	71.27%	48.32%
Avast!	7.49%	7.22%	95.26%	1.21%
Avertive	3.45%	2.55%	9.02%	12.25%
AVG	6.45%	6.75%	84.58%	2.97%
Avira	3.15%	2.73%	22.23%	7.49%
BitDefender	4.09%	5.23%	36.07%	24.91%
BullGuard	4.40%	3.23%	45.64%	65.52%
Central Command	4.11%	4.49%	43.05%	19.35%
Clearsight	4.95%	5.10%	53.05%	12.37%
CommTouch	5.57%	5.16%	163.00%	119.93%
Comodo AV	5.50%	5.54%	61.18%	0.40%
Comodo IS	6.87%	6.73%	67.70%	0.17%
Coranti Cora	8.36%	8.06%	43.29%	17.47%
Defenx	7.79%	8.64%	92.77%	62.99%
Digital Defender	5.70%	5.77%	74.14%	12.35%
eEye	7.41%	6.96%	112.13%	3.98%
Emsisoft	1.03%	2.39%	54.27%	21.30%
eScan	2.19%	3.12%	22.28%	8.00%
ESET	5.75%	6.04%	41.94%	11.79%
ESTsoft	3.20%	4.41%	32.19%	20.78%

<b>Performance measures</b>	Idle RAM - usage increase	Busy RAM - usage increase	Busy CPU - usage increase	Standard file activities - time increase
Fortinet	6.44%	5.39%	84.20%	16.96%
Frisk	5.44%	4.92%	62.60%	-3.42%
F-Secure	6.01%	6.18%	82.61%	2.39%
G Data	7.15%	8.42%	83.21%	10.36%
GFI	3.96%	4.40%	73.92%	3.28%
Hauri	2.48%	2.67%	13.38%	3.05%
Iolo	4.91%	4.16%	158.96%	120.14%
Kaspersky	4.32%	3.81%	33.04%	2.93%
Lightspeed	3.07%	3.66%	1.69%	3.72%
Lumension	20.79%	20.85%	110.37%	18.35%
Microsoft	4.13%	4.48%	55.74%	2.59%
Norman	37.00%	30.67%	111.86%	11.36%
Preventon	5.89%	6.13%	82.93%	14.71%
Quick Heal	10.63%	10.26%	71.87%	15.16%
Returnil	5.00%	4.12%	153.50%	62.52%
Rising	0.96%	1.47%	56.62%	30.51%
Sophos	6.00%	6.41%	63.86%	6.43%
SPAMfighter	4.72%	4.97%	51.96%	12.38%
TGSoft	2.50%	2.60%	23.45%	2.07%
Total Defense	9.76%	10.46%	7.52%	122.38%
UtilTool	6.18%	5.90%	90.82%	45.74%
VirusBuster	4.11%	4.49%	43.05%	19.35%

(Please refer to text for product names.)



(Please see text for full product names.)



*(Please see text for full product names.)*

while others look all new but are immediately clear and easy to operate. Testing thus moved along nicely.

Speeds were a little sluggish in initial scans, but the warm runs powered through much more rapidly thanks to some smart optimization. On-access overheads were distinctly on the light side. Resource use was low and our set of standard activities ran through very quickly indeed. Detection tests were mostly completed with ease, although a few parts of the RAP sets did seem to cause some rather lengthy hangs, and we re-ran them just to be safe, seeing no repeat of the slowdowns. Scores were very solid across the sets, with a very good showing in the RAP sets, tailing off only slightly into the latter weeks, while the Extended WildList was perfectly handled on demand, only the *Android* items being ignored by the real-time component. The core certification sets presented no difficulties at all, and a VB100 award is comfortably earned by *Kaspersky*.

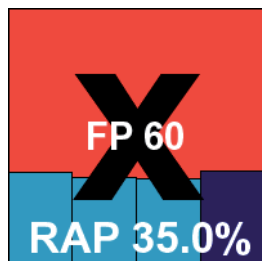
The company’s history is a little diverse given its wide product range, but counting this fully fledged suite as part of the *Internet Security* continuum, we see four passes from five attempts in the last six tests; nine from ten in the last two years. With good reliability and splendid speeds, even with a few re-runs to double-check things, all tests were completed within the allotted 24 hours.

### Lightspeed Systems Total Traffic Control 8

Version 8.01.04

<b>ItW</b>	81.95%	<b>Worms &amp; bots</b>	57.65%
<b>ItW (o/a)</b>	81.95%	<b>Polymorphic</b>	94.86%
<b>Extd. WL</b>	65.33%	<b>Trojans</b>	64.78%
<b>Extd. WL (o/a)</b>	65.33%	<b>False positives</b>	60

Another newcomer to our comparatives, we have been in contact with *Lightspeed Systems* for some time but have only now managed to get the product included in a test. The company’s main market is apparently in the US education system; its product is entirely the company’s own work with no OEM technology included. The installer submitted was a slim 13MB package, which we installed and updated online on the deadline day. The set-up process was fast and simple, with only a couple of clicks required and all done in under half a minute with no request for a reboot.



With installation complete, we tried opening the interface to no avail. A reboot sorted this out however, and we got our first look. The layout looked decent, clear and simple to use,

and provided a reasonable degree of control, but updating seemed to take some time, the progress bar halting on 10% and staying there for over an hour. Another reboot and retry of the update did the same, but leaving it going finally produced results and we were able to continue.

Using the product was generally no problem, and we produced speed and performance stats showing fairly slow on-demand scanning speeds but very light overheads on access and low resource use, with little effect on our suite of tasks. Closer examination showed that this was probably mainly a result of the real-time protection not being applied on read by default, and our detection tests were thus run by copying files around the system rather than using our usual opener tool. In the larger tests, stability under pressure was rather suspect, with scans taking a long time to return control after completion. This proved to be the case even when scanning clean samples only, with the scan of our clean sets leaving the system completely unresponsive for over four hours. It appears that the product records all unknown files as well as those flagged as detected – presumably as part of some sort of whitelisting system – so perhaps these odd slowdowns are due to trying to feed this data back to some remote server, inaccessible from our lab environment.

Results were eventually obtained, and were a little disappointing, with a fairly large number of misses in most areas. RAP scores were poor, but fairly even across the weeks at least, and in the WildList set quite a number of items were undetected. In the clean sets there were also quite a few false alarms, including files from major brands such as *Adobe* and *Acer* as well as components of popular software like *Alcohol*, *Azureus/Vuze*, the *Steam* gaming system, and *EASEUS Partition Master*. All of this means, of course, that *Lightspeed* will need to do quite a bit more work to meet our certification requirements, although it seems to have made a fairly decent start. With the slow scans and long recovery times, testing took around a week to complete.

### Lumension Endpoint Management and Security Suite

Scan engine version 6.7.10, Antivirus definition files 6.7

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	90.16%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.98%
<b>Extd. WL</b>	99.82%	<b>Trojans</b>	93.33%
<b>Extd. WL (o/a)</b>	99.82%	<b>False positives</b>	0

Another product from the whitelisting field, *Lumension* has a previous pass under its belt thanks to the *Norman* engine bundled with its heavyweight corporate solution. However,

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost	OD	1	√	√	√	√	X	√	X	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
AhnLab V3Net	OD	9	9	9	9	9	9	9	X	9	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ArcaBit ArcaVir	OD	2	√	√	√	√	√	√	√	√	1	√
	OA	2	√	√	√	√	√	√	√	√	1	√
Avast Free Antivirus	OD	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
	OA	X/√	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/√	√
Avertive VirusTect	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
AVG IS	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Avira AntiVir Server	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/√	√
BitDefender Security	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/√	X/√	4/√	4/√	8/√	X/√	X/√	X/√	X/√	X/√	X/√
BullGuard Antivirus 10	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	2	2	2	1	2	2	2	1	2	2	√
Central Command Vexira	OD	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Clearsight Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
CommTouch Command	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	2/4	2/4	2/4	2/4	2/4	√	2/4	1/2	2/4	2/4	√
Comodo Antivirus	OD	X	5	5	5	5	5	5	2	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Comodo IS	OD	X	5	5	5	5	5	5	2	5	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√

Key:

√ - Detection of EICAR test file up to ten levels of nesting

X - No detection of EICAR test file

X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

\* Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names.)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Coranti Cora	OD	√	√	X	X	√	√	√	8	1	√	√
	OA	X/1	X	X	X	X/√	X	X	X	1	X/1	X/√
Defenx Security Suite	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	√	√	√	√	X	√	√	√	X	√
Digital Defender	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
eEye Blink Server	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	X	X	X	X	X	X	X	X	X	X	X/√
Emsisoft Anti-Malware	OD	√	7	6	5	7	7	7	7	8	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
eScan IS	OD	√	√	√	√	√	√	√	5	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ESET NOD32 Antivirus	OD	X	X	8	8	X/√	X/√	X	X	X/√	X	√
	OA	X	X	8	8	X	X	X	X	X	X	√
ESTsoft ALYac	OD	X	1	1	1	1	1	1	8/√	2	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	√	√	√
	OA	X	√	√	√	√	√	√	√	√	√	√
Frisk F-PROT	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	2	2	X	X	X	2	2	√
F-Secure Anti-Virus	OD	X/√	√	√	√	√	√	√	8	√	X/√	X/√
	OA	X/√	X/√	X/√	X/√	X/√	X/√	X/√	X/8	X/√	X/√	X/√
G Data AntiVirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	√	√	√	√	√	√	√	√	√
GFI VIPRE Antivirus	OD	X	X	√	√	√	X	√	X	√	X	√
	OA	X	X	√	√	X	X	X	X	X	X	√
Hauri ViRobot Server	OD	X	X/5	X	X	X/5	X/5	X/5	X/2	1/6	1	√
	OA	X	X	X	X	X/√	X	X	X	X/1	X/1	X/√
Iolo System Shield	OD	5	5	5	5	5	√	5	5	5	5	√
	OA	5	5	5	5	5	√	5	5	5	5	√

## Key:

√ - Detection of EICAR test file up to ten levels of nesting

X - No detection of EICAR test file

X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

\* Detection of EICAR test file with randomly chosen file extension

(Please refer to text for full product names.)

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Kaspersky Endpoint Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Lightspeed TTC	OD	X	√	√	√	√	X	√	8	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Lumension EMSS	OD	X	√	√	1	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Microsoft Forefront	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√
Norman Endpoint Protection	OD	X	√	√	1	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Preventon Antivirus Server	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
Quick Heal	OD	X/2	2/5	X	X	2/5	X	2/5	1	2/5	X	X/√
	OA	2	X	X	X	1	X	X	X	1	X	√
Returnil System Safe	OD	5	5	3	2	5	7	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Rising Internet Security**	OD	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	OA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Sophos ESC	OD	X	5	5	5	5	5	5	5	5	5	√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
SPAMfighter VIRUSfighter	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	X/1	X/1	X	X	X/1	X	X/1	X	X/1	X/1	X/√
TGSoft VirIT eXplorer	OD	X	X	X	X/√	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Total Defense r12	OD	X	X/√	X/√	X/√	√	X/√	X/√	X/√	√	X/√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
UtilTool Server Antivirus	OD	1	1	X	X	1	X	1	X	1	1	√
	OA	1	1	X	X	X/1	X	1	X	1	X/1	X/√
VirusBuster	OD	2	√	√	√	X/√	X	√	√	√	X/√	X/√
	OA	X	X	X	X	X	X	X	X	X	X	X/√

Key:

√ - Detection of EICAR test file up to ten levels of nesting

X - No detection of EICAR test file

X/√ - default settings/all files

1-9 - Detection of EICAR test file up to specified nesting level

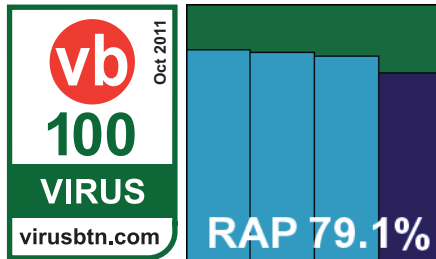
\* Detection of EICAR test file with randomly chosen file extension

\*\* No apparent detection of EICAR test file

(Please refer to text for full product names.)



it made no friends in its last appearance with a distinctly difficult interface and some odd approaches to implementation.



Set-up

from the 198MB bundle included the provision of several dependencies, including *Microsoft's Silverlight*, .NET framework and an upgrade to the installer system, which took around 15 minutes, requiring a reboot before we could continue with the installation proper. On attempting this, we discovered yet more requirements, including the activation of IIS and ASP, which had to be done via the server management system. Moving on again, we ran through a more standard install process which, after gathering some information, took around 20 minutes to complete.

The product interface is web-based and suffers the expected flakiness, sluggish response, frequent freezes and session timeouts we have come to associate with such control systems. An often bewildering layout, complex procedures for performing simple tasks, and a scanning system which lacks a simple 'scan' option were all additional frustrations that led to considerable wailing and gnashing of teeth in the test lab before we were done with this one. On-demand speed tests were performed using the only option available: an entire system scan with the option to exclude certain areas. To get just the folders we required scanned, we had to add a lengthy list of such exclusions using a fiddly XML format, but we soon got the hang of it and seemed to be moving along. We then discovered a bug in the exclusion system, which meant that once an item had been added to the exclusion list it could not be removed; although the interface reported successful removal and showed a shorter list, at the end of a scan it had reappeared in the list hidden away in the scan log. This meant multiple retries, taking huge amounts of time as the scanner seemed to check each file on the entire system in turn, only to ignore most as the partition they were on was excluded.

We did eventually persuade it to scan through our speed sets alone, but the additional overheads meant the times were extremely slow, barely even visible on our graph. It seems that the scanner design overheads were not the sole cause of this slowness though, as the on-access lag times were extremely heavy too, with high use of memory and processor cycles throughout and a noticeable impact on our suite of activities.

Detection tests were similarly troublesome, with several attempts once again hampered by the misfiring exclusion

system, and those which did get started regularly stopped silently after only a fraction of the job, with no reason given for the abort. Having gone away to the VB conference leaving it running over the full sets once more, we returned to find data for only the first few days of the first set, and yet more retries were needed. With time pressing, the RAP data was harvested using the on-access component, which seemed to be more reliable but may not have provided the full detection capabilities of the barely usable on-demand scanner.

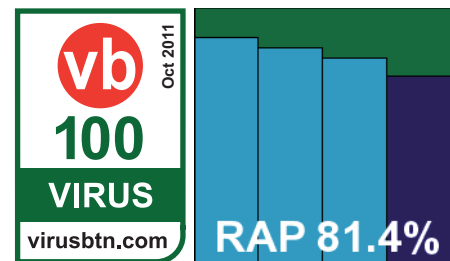
In the end, detection rates were respectable, with a good showing in the main sets and slightly lower scores through the RAP sets, although some of the scores here were actually slightly higher than those recorded by other entries using the same engine. In the Extended WildList just a couple of *Android* items in archive formats were ignored, and the standard list was covered well. With no false alarms in the clean sets, *Lumension* just about scrapes a VB100 award, having made our lives extremely difficult once again. From two entries the company now has two passes, and thanks to the design of the product as much as the bugs in the scan set-up system and the scanner itself, testing took up one of our test machines for more than three full weeks.

## Microsoft Forefront Endpoint Protection

Product version 2.1.1116.0, Signature version 1.111.469.0

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	96.09%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	92.40%
<b>Extd. WL (o/a)</b>	99.82%	<b>False positives</b>	0

Back to a company with a slightly more standard approach to GUI design, *Microsoft's* corporate product was submitted



as a svelte 20MB installer with just 64MB of additional updates, and the set-up process was simple and speedy with no reboot required. The interface is pretty familiar to us by now, looking clean and sharp, providing only basic controls and occasionally confusing with its use of language but proving generally fairly usable.

Scanning speeds were pretty reasonable, and overheads light, with low RAM use and impact on our set of activities, and busy CPU use around average. Detection

tests ran through smoothly if a little more slowly than the ideal, showing some solid scores across the board with a very even downward slope through the RAP sets. The Extended WildList set saw everything blocked on access, while processing on-demand logs using our standard method showed two items not detected. Closer analysis showed that these were in fact both alerted on, one as a ‘Hack Tool’ and the other labelled ‘Remote Access’. These ‘grey’ type detections are not counted under our current scheme but are likely to be included once the new set becomes part of the core requirements – although we would hope that such borderline items will be excluded from the list at an earlier stage in future. The core certification sets were well handled, and a VB100 award is comfortably earned.

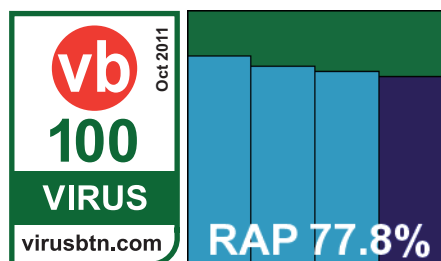
*Forefront’s* test history is solid if sporadic, the company alternating entries with its consumer offering. From three entries in the last six tests, three passes have been attained; five passes from five tries in the last two years. Testing ran without incident but detection tests were a little slow, all jobs completing in around two full testing days.

### Norman Endpoint Protection

Program Manager version 8.10, Scan engine version 6.07.10, Antivirus version 8.10

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	90.30%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.98%
<b>Extd. WL</b>	99.18%	<b>Trojans</b>	93.42%
<b>Extd. WL (o/a)</b>	99.82%	<b>False positives</b>	0

Yet another of our old-time regulars, whose engine has already cropped up a few times this month, *Norman’s* current product came as a



131MB installer including all updates, and set up in half a dozen standard steps, running at average speed and needing no reboot. The interface remains rather clumsy and less than reliable, prone to regular freak outs, freezes and general flakiness – including occasionally going all blurry, much to our consternation. The layout is often confusing, and only manages to provide a limited selection of configuration controls even after considerable searching. We also noted that it regularly ignored our instructions, deleting and disinfecting items having explicitly been told to log only.

Nevertheless, tests proceeded reasonably well, with the expected crawling scan speeds and hefty on-access overhead. RAM and CPU use were pretty high but our set of tasks did not take too much longer than normal to get through. Detection tests were completed without too much effort, showing some pretty decent scores in most areas, with the Extended WildList dealt with fairly well on access, only a couple of non-standard file types ignored, while on demand a handful of executables were omitted. Looking deeper, we saw that the missed files were all consecutive, hinting that some chunk of the files had been passed over, or a problem with logging had occurred. The main WildList and clean sets were handled properly, earning *Norman* a VB100 award.

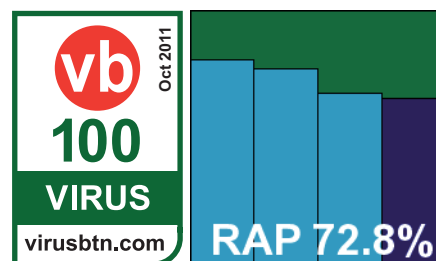
The vendor’s test history shows five passes from the last six tests – a great improvement on the previous year as we see only six passes from 11 attempts over the last two years. With considerable flakiness of the interface, the actual protection seemed to be pretty stable, but slow scanning speeds added to testing time, and all jobs completed after about three days.

### Preventon Antivirus Server

Version 5.0.69, Definitions version 14.0.179

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.76%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	90.34%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0

The source of a number of entries this month, *Preventon* promised few surprises. Setting up the product from its 68MB installer – which ran through in good time with no reboot – and using the interface, which is simple and clear with a good basic level of controls, proved something of a breeze. Logging remains the main headache with this product, with registry tweaks required to prevent it dumping records after a few MB.



Speed tests showed slowish scan times and lightish overheads, with resource use perhaps a shade above average and impact on our set of tasks likewise slightly on the high side. Detection tests ran through without problems, showing some reasonable scores across the board, a fair few misses in the Extended WildList but no problems in the main list or clean sets, earning the product another VB100 award without fuss.

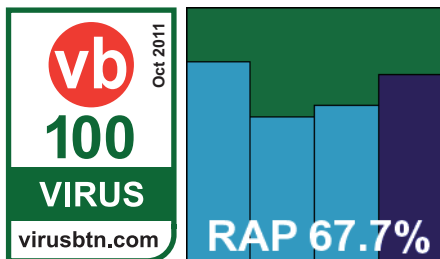
The vendor’s test history shows four passes from five entries in the last six tests; six from eight attempts in the last two years. Testing was all plain sailing, taking just a little more than the 24 hours allotted.

### Quick Heal AntiVirus Server Edition

Version 13.00 (6.0.0.1)

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	90.82%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.45%	<b>Trojans</b>	90.04%
<b>Extd. WL (o/a)</b>	99.73%	<b>False positives</b>	0

*Quick Heal’s* ‘Server Edition’ came as a 228MB bundle, which ran through in quite good time for the size, with no reboot needed.



The interface is pretty much identical to consumer versions we’ve seen in recent tests: clean and modern with a few slight quirks of layout, but fairly good usability and clarity.

Testing ran through very nicely, with scanning speeds not too slow, notably higher over executables than elsewhere, and overheads a little high, but lighter on executables. Resource use was unremarkable with most measures around average. Detection rates were pretty strong on demand, noticeably lower on access, but RAP scores were rather unpredictable, dipping after a decent start but then climbing upward again into the latter weeks. The Extended WildList showed a handful of ignored items, but the core certification requirements were met without difficulty and a VB100 award is duly earned.

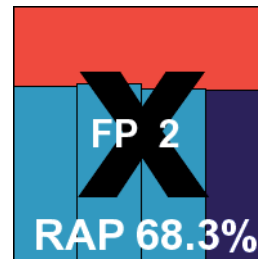
The company’s history in our tests goes back almost a decade, and has been pretty strong of late, with six passes in the last six tests; 11 passes and a single fail in the last two years. Testing ran smoothly this month with no major errors, all completing on schedule in under a day.

### Returnil System Safe 2011

Version 3.2.12918.5857-REL14

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	74.55%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	81.68%
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	2

Another OEM product, this one uses the *Frisk* engine by way of *CommTouch* alongside its own speciality, a virtualization and reversion system to undo unwanted changes to a system before they can be permanently committed. The installer measured 38MB, with updates in a separate 28MB bundle. The set-up process was speedy with little attention required, although a reboot was demanded at the end.



The interface looks pretty decent and provides simple access to a basic range of controls (once again context menu scanning is notable by its absence), and it ran pretty stably throughout testing. Scanning speeds were slow and overheads pretty high, with low RAM use but high use of CPU and a fairly heavy effect on the runtime of our standard activities, as noted with other products based on the same technology. Detection rates were unremarkable, apart from a very steady base rate across the RAP sets, and the traditional WildList set was well handled. In the clean sets, as feared, the same file from a driver CD caused an alert, and a second clean file was also wrongly flagged as infected. This was enough to deny *Returnil* certification this month despite an otherwise decent showing.

The product now has three passes from five tries in the last six tests; four passes and three fails overall. Testing was a little slow but there were no serious issues, all completing in around a day and a half of test lab time.

### Rising Internet Security

Version No.: 23.00.41.88

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	N/A
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	N/A
<b>Extd. WL</b>	99.36%	<b>Trojans</b>	N/A
<b>Extd. WL (o/a)</b>	99.45%	<b>False positives</b>	6

*Rising’s* latest product gave us some problems last time around but just about scraped a pass, and we hoped to see some improvements in stability and general sanity this month. The installer measured 89MB including all updates, and ran through fairly speedily although with a fair few clicks required. The interface is distinctly unusual, both in layout and general look and feel, with a sparkly colour scheme and a home page dominated by performance graphs. Navigation can be baffling at times, mainly thanks to oddities of translation, but a reasonable level of configuration appears to be available for those able to fathom its mysteries.

Initial testing proceeded well enough, with slow scanning speeds apart from the warm scan of archives, light overheads and low RAM use, CPU use around average and impact on our set of tasks around average. Detection tests were rather painful though, with once again huge issues with the logging and reporting system. Scans repeatedly ran along merrily racking up thousands of detections, only to come to an end with a message stating ‘No virus was founded’ [*sic*] and ‘Your computer security is safe’. Picking as much as we could out of logs, and re-running scans carefully multiple times, we still found no reliable data, and once again had to give up under time pressure. Thus no RAP scores or detection rates for several of the main sets were available, but at least we managed to get through the WildList sets, which showed solid coverage, including complete detection of the Extended list on demand. In the clean set, however, a number of false alarms were noted, including an item from *Sun* labelled as a dropper trojan, and as a result no VB100 award can be granted to *Rising* this month.

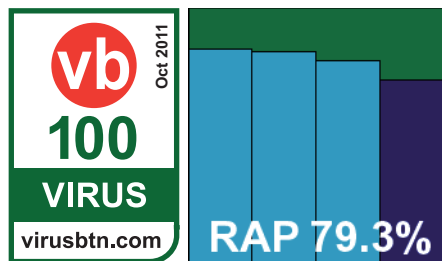
The company’s test history shows sporadic entries in our comparatives, with one pass and two fails in the last six tests; three of each in the last two years. With all the reporting issues and multiple retries needed, testing ran for over two weeks before we gave it up as a lost cause.

### Sophos Endpoint Security and Control 9.7

Sophos Anti-Virus 9.7.4, Detection engine 3.22.0, Detection data 4.68G

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	79.64%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	81.80%
<b>Extd. WL (o/a)</b>	99.91%	<b>False positives</b>	0

The current version of *Sophos*’s standard *Windows* desktop product comes as an 89MB installer, with additional incremental updates measuring just a few hundred KB. The install process has perhaps a few more stages than average but is done with in good time, needing no reboot to complete. The interface is stark and functional but fairly simple to operate, providing the full range of controls one would expect from an enterprise-grade solution, including



extreme fine-tuning in a super-advanced area. Testing ran through without any nasty surprises.

Scanning speeds were a fraction above average, but so were on-access overheads, with resource use and impact on our set of tasks unexceptional. Detection tests showed some respectable if not stellar scores, with flawless coverage of the Extended WildList. The traditional list and clean sets were also handled impeccably, comfortably earning *Sophos* a VB100 award.

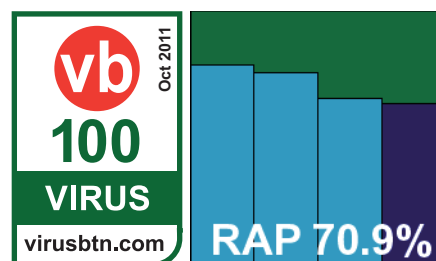
The vendor’s recent test history is similarly impeccable, with 12 passes in the last two years; this month’s testing revealed no problems, and completed in just slightly over the recommended 24 hours.

### SPAMfighter VIRUSfighter PRO

Version 7.0.258

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	88.63%
<b>ItW (o/a)</b>	100.0%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	88.99%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0


















The *VIRUSfighter* brand included the *Norman* engine when we first encountered it, but for the last few years it has



been part of the *Preventon* family, albeit with a little more of the vendor’s own work put into the design than most. The installer measured 66MB, and set-up was simple and rapid. The interface is cleaner and more obvious in its controls than early versions, but still provides a decent basic level of configuration.

















Logging remains an issue, with logs capped at a fixed size and, in this case, no clear way of changing them. By default, all files scanned are written to logs (although this can be changed with a registry tweak), so any malware spotted before the last few thousand files of any scan would not be remembered by the product. Even the sloppiest of server admins would be unlikely to countenance such a lack of accountability in a product, but it may be OK for home users who rarely seem to care much about what their security products get up to.

Speed tests showed reasonable throughput and lag times, with average use of resources and not too much effect on our set of tasks. Detection rates on demand were gathered by mounting the log folder on a remote system and backing

Reactive And Proactive (RAP) scores	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		81.89%	81.11%	72.74%	78.58%	67.14%	75.72%
AhnLab V3Net		83.12%	80.36%	74.34%	79.27%	69.83%	76.91%
ArcaBit ArcaVir*		NA	NA	NA	NA	NA	NA
Avast! Free Antivirus		96.27%	94.31%	89.21%	93.26%	79.69%	89.87%
Avertive VirusTect		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
AVG Internet Security		95.79%	93.52%	85.93%	91.75%	74.39%	87.41%
Avira AntiVir Server		98.65%	97.69%	92.49%	96.27%	86.38%	93.80%
BitDefender Security for File Servers		97.79%	97.69%	95.73%	97.07%	87.75%	94.74%
BullGuard Antivirus 10		97.72%	97.44%	95.31%	96.82%	87.29%	94.44%
Central Command Vexira		80.17%	79.18%	70.60%	76.65%	64.82%	73.69%
Clearsight Antivirus		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
CommTouch Command		67.81%	68.85%	66.73%	67.80%	66.41%	67.45%
Comodo Antivirus		88.31%	82.23%	76.72%	82.42%	69.99%	79.31%
Comodo Internet Security		88.31%	82.23%	76.72%	82.42%	69.99%	79.31%
Coranti Cora Antivirus		64.81%	67.61%	67.74%	66.72%	66.32%	66.62%
Defenx Security Suite 2012		82.24%	81.45%	73.33%	79.00%	67.59%	76.15%
Digital Defender		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
eEye Blink Server		81.23%	77.43%	75.36%	78.01%	73.12%	76.79%
Emsisoft Anti-Malware		98.78%	98.38%	96.73%	97.96%	86.69%	95.14%
eScan Internet Security		97.75%	97.40%	94.00%	96.38%	86.32%	93.87%
ESET NOD32 Antivirus		94.40%	92.04%	91.35%	92.60%	84.50%	90.57%
ESTsoft ALYac		96.83%	96.20%	92.47%	95.17%	84.95%	92.61%

\* Testing not possible

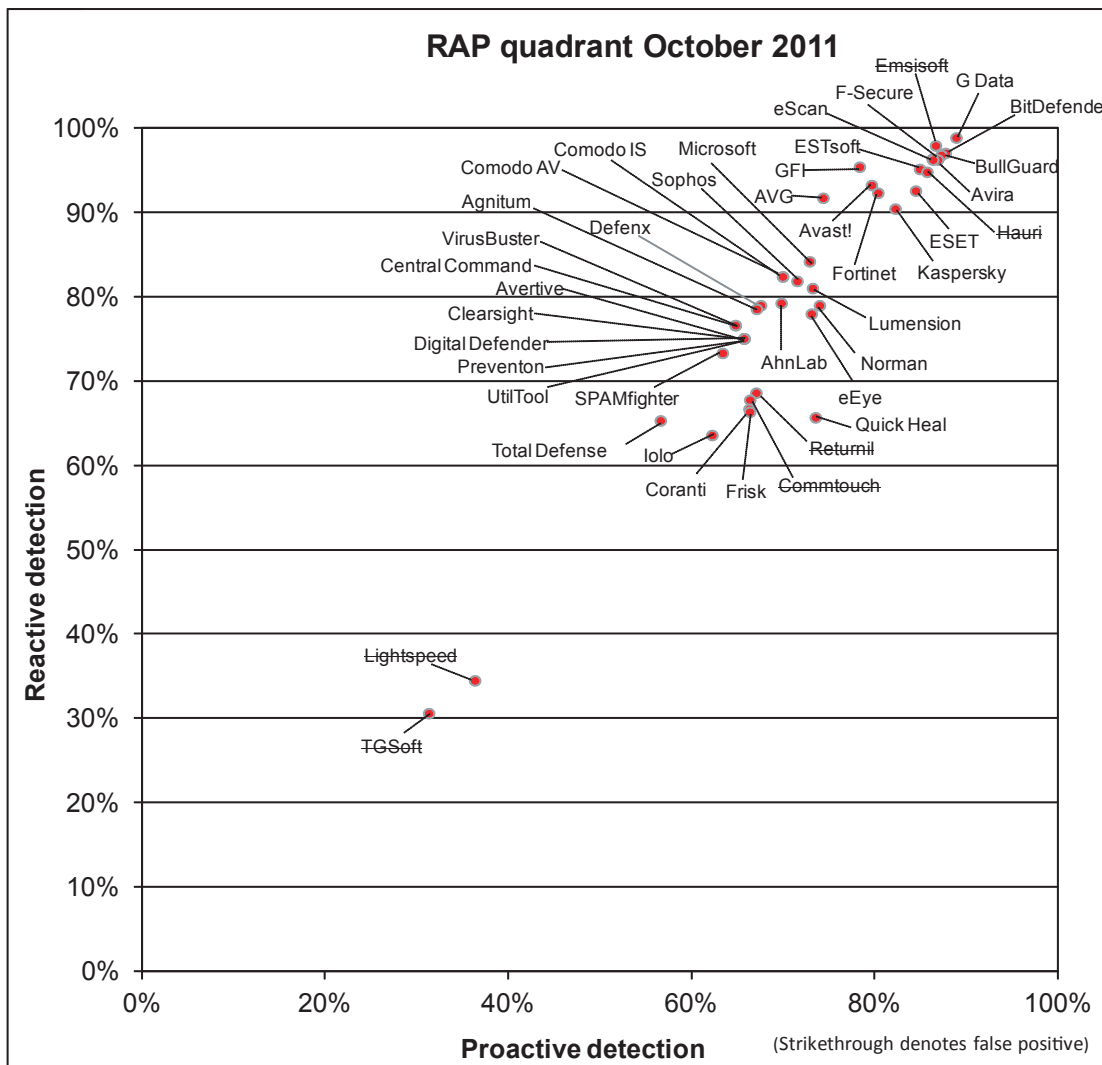
(Please refer to text for full product names.)

Reactive And Proactive (RAP) scores	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Fortinet FortiClient		93.58%	92.79%	90.67%	92.35%	80.39%	89.36%
Frisk F-PROT		64.90%	67.69%	66.52%	66.37%	66.39%	66.38%
F-Secure Anti-Virus**		97.24%	97.36%	94.27%	96.29%	86.92%	93.95%
G Data AntiVirus		99.72%	99.64%	97.32%	98.89%	88.92%	96.40%
GFI VIPRE Antivirus		97.94%	98.03%	90.32%	95.43%	78.37%	91.17%
Hauri ViRobot Server		95.85%	95.10%	93.54%	94.83%	85.75%	92.56%
Iolo System Shield		63.90%	64.71%	62.22%	63.61%	62.27%	63.28%
Kaspersky Endpoint Security 8		93.04%	88.88%	89.49%	90.47%	82.27%	88.42%
Lightspeed Total Traffic Control		36.00%	33.89%	33.66%	34.52%	36.37%	34.98%
Lumension EMSS**		82.10%	81.34%	79.68%	81.04%	73.25%	79.09%
Microsoft Forefront		88.35%	84.17%	80.12%	84.21%	72.92%	81.39%
Norman Endpoint Protection		82.31%	78.33%	76.38%	79.01%	74.02%	77.76%
Preventon Antivirus Server		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
Quick Heal		78.78%	56.79%	61.56%	65.71%	73.57%	67.68%
Returnil System Safe		68.66%	69.67%	67.57%	68.63%	67.08%	68.25%
Rising Internet Security*		NA	NA	NA	NA	NA	NA
Sophos Endpoint Security and Control		83.76%	82.57%	79.34%	81.89%	71.56%	79.31%
SPAMfighter VIRUSfighter PRO		78.84%	75.74%	65.48%	73.35%	63.42%	70.87%
TGSoft VirIT eXplorer		30.17%	29.62%	32.07%	30.62%	31.35%	30.80%
Total Defense Inc Total Defense r12		70.77%	65.44%	59.82%	65.34%	56.64%	63.17%
UtilTool Server Antivirus		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
VirusBuster for Windows Servers		80.17%	79.18%	70.60%	76.65%	64.82%	73.69%

\* Testing not possible

\*\* On-demand scanner not testable, on-access data used

(Please refer to text for full product names.)



(Please refer to text for full product names.)

up the backup file each time it changed. On access, an initial scan ran into problems when the screensaver came on, which seemed to trip up the scanner, leaving the run frozen. A reboot was needed to get things moving again, this time with the screensaver disabled. Final results showed the expected decent but not remarkable scores across the board, with a reasonable showing in the RAP sets and no issues in the core certification sets.

SPAMfighter thus earns another VB100 award, the vendor's fourth from five tries in the last six tests. Its longer term history shows five successes from eight entries in the last two years. The screensaver upsetting the on-access scanner was the only problem noted, and testing took around a day and a half to complete.

### TGSoft VirIT eXplorer Pro

Version 6.9.70

<b>ItW</b>	47.51%	<b>Worms &amp; bots</b>	40.19%
<b>ItW (o/a)</b>	47.30%	<b>Polymorphic</b>	68.48%
<b>Extd. WL</b>	31.12%	<b>Trojans</b>	23.29%
<b>Extd. WL (o/a)</b>	31.12%	<b>False positives</b>	3

Another relatively fresh face, TGSoft first took part in a VB100 test a few months ago, and despite getting rather a pasting bravely returns for more this month. The product is by far the smallest in this test, with the main installer measuring 16MB and updates just 5MB. Although the

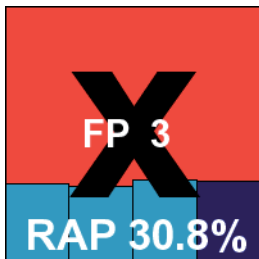
set-up process has a fair number of steps to click through and needs a reboot at the end, it is done with in very good time.

The interface is distinctly retro, very basic and simplistic, but does provide a few useful controls for those with the ancient knowledge of how to operate them.

Stability was generally pretty decent, and scan times were good, with fairly light overheads and low use of resources. Our set of tasks zipped through in good time too, barely slower than the baseline measure.

Detection rates, on the other hand, remain pretty low, with quite some work to do in most areas. The WildList was not handled completely disastrously though, and with only a handful of false positives things certainly seem a little better than last time.

If improvements continue at this rate, we could well see the product qualifying for certification within the next couple of years. There were no bugs or errors uncovered during testing, and with good speeds everything completed in short order, in less than a day.



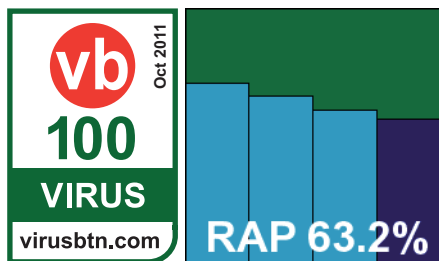
### Total Defense Inc. Total Defense r12

Product version 12.0.528

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	79.25%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	99.96%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	81.82%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

*Total Defense* looks set to become a regular name in our tests, with CA now no longer associated with the product range.

The business edition has proven somewhat pesky in the past, but things seem to grow easier with practice (although never quite reaching normal standards). Initial dependencies include the .NET framework – indeed a specific version thereof, as we discovered after installing the most recent one (a process which included a reboot) and having it rejected by the product installer. The set-up process, run from a DVD image on the deadline day, also includes a fair number of data-collection screens, some



of which are quite poorly thought through. For example, after specifying that I live in the UK, I was still required to select from a list of US states as part of my personal details. After finishing the main set-up and rebooting, an online update took place, which took around half an hour, then demanded yet another reboot.

The interface itself is fairly pleasant and usable, now that we have dispensed with the need to look upon the horrors of the central management system, and most of the testing ran through quite nicely. Scanning speeds were very fast and overheads low, and although RAM use was a little higher than average, CPU was pretty low at busy times. This may in part be due to the way our CPU measures are recorded, with multiple snapshots taken throughout the performance measure period; while most products remain active throughout this time, in this case the activities took a very long time to complete, during much of which the product was apparently idle.

On-demand scans once again store data in memory, resulting in huge amounts of memory use and slow and flaky scans, so as usual we had to split things up into smaller chunks, but still had to sit through some long, slow, nail-biting jobs. With all data eventually in, we saw some respectable scores in the main sets, with RAP scores dropping off quite severely. The Extended WildList was properly dealt with however, and with no issues in the main list or clean sets *Total Defense* earns a VB100 award.

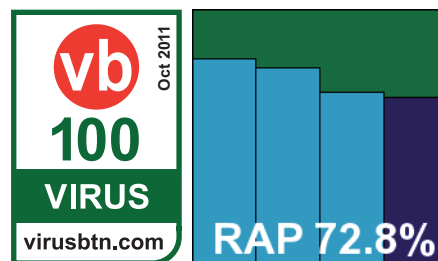
The product, regardless of its owners, now has four passes from five attempts in the last year; seven from ten in the last two years. Testing this month ran fairly smoothly, but the slow detection tests meant that more than three days of lab time were needed to get things done.

### UtilTool Server Antivirus

Version 2.1.69, Definitions version 14.0.179

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.76%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	92.54%	<b>Trojans</b>	90.34%
<b>Extd. WL (o/a)</b>	92.45%	<b>False positives</b>	0

One of the freshest branches to spring from the *Preventon/VirusBuster* tree, we don't know much about *UtilTool*,



other than that the company appears to hail from Eastern



Europe (judging by the Russian and Ukrainian options on its website). The ‘server’ version of the product, which is remarkably similar to desktop editions from the rest of the family, came as a 67MB package, with the usual fast and simple install and basic but usable interface. We’ve commented already on logging problems, and also on a few odd signs of instability in what has traditionally been a pretty reliable solution, and here again we had a moment of madness – shortly after installation, the test machine suddenly lost track of all its search paths, rendering it basically unusable, and on reboot a full consistency check was needed to repair things. No further freak outs occurred though, and the rest of testing moved along nicely.

Scanning speeds were average, and overheads a little heavier than expected, with lowish use of RAM but fairly high use of CPU and a noticeable hit on the speed of our set of tasks. Detection rates were as expected though, with decent coverage across the sets, no problems in the core sets and the requirements for VB100 certification met at first attempt.

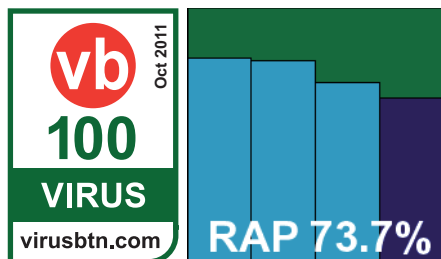
Other than the single crazy moment with the search paths, no major issues were observed, and with reasonable run times, testing took only a little more than the day set aside for the product.

### VirusBuster for Windows Servers

Product version 7.1.76, Scan engine 5.3.0, Virus database 14.0.183

<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	89.10%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	99.45%	<b>Trojans</b>	90.75%
<b>Extd. WL (o/a)</b>	98.91%	<b>False positives</b>	0

The daddy of them all, I think it is safe to say that the *VirusBuster* engine has had a pretty thorough workout this



month, in its various guises. Even the interface has been gone over before, in the form of *Vexira*, and here it is again with just a few tweaks to the colour scheme. As in that case, the installer is 67MB, with 61MB of updates, and set-up is uncomplicated and fairly zippy, needing a reboot to finish.

We have seen relatively few MMC-based interfaces this month – for which we are eternally grateful, as they

generally tend to be awkward and uncomfortable, much as this one is. The layout is at least reasonably simple to navigate after a few hours of careful exploration, but the lack of consistency and general clumsiness renders it less than a pleasure to operate. Stability was not a problem though, and tests ran to completion without incident.

Speeds were average, overheads a little above the norm, with resource use similarly unremarkable and our set of tasks taking perhaps a little longer here than most runs this month. Detection rates barely merit comment, being just as the rest of the crop – decent but unlikely to challenge the very best. The core sets were well handled though, and a VB100 is duly earned.

The company’s recent test history is good, with six passes in the last six tests; 11 from 12 attempts in the last two years. With no major issues, testing overran the anticipated 24 hours only slightly.

### CONCLUSIONS

Another rather epic test, not in terms of the number of products entered but rather in the time taken to get through them all. This report is finally approaching completion, close to a month *after* our expected deadline. Of course, in part this is due to the lab team having been taken away from their screens by both the *VB* conference and some other important industry meetings – but had things gone to plan, all of the testing would have been complete and most of the processing out of the way before we headed away for our trips.

For the most part, products were well behaved and got through the testing in good time. Admittedly several did overrun a little, but had we set our expectations a little lower, granting each product two full days of testing time, all but a dozen or so would have comfortably made it. Those last, however, were for the most part extremely troublesome, not overrunning by just a few hours or even days, but in several cases needing weeks of precious system time. Indeed, in several cases we had to abandon products with little to show for a great number of man hours dedicated to getting something usable out of them.

The main problem with these products is stability, which in turn can be attributed to a lack of proper quality control prior to release. A large number of the problems we’ve seen here should be showstoppers in any product release cycle, and we continue to be amazed by how many products can go to market with serious problems which really need to be resolved before they are inflicted on unwitting, and of course paying, customers. Hopefully this report will help guide at least some would-be purchasers

away from the more dangerously unstable products, as well as encourage vendors to be more thorough in their QA procedures.

Of course it's not all bad, and we've seen some sterling performances as always – for the most part from the select elite who routinely excel in our tests, but also in a few cases from fairly new faces. One entirely new name has been added to the roster of certified solutions, having put in an impressively solid showing.

Now it is time to move forward, towards our all-new, rather different testing procedure. As we have seen this month, the new Extended WildList seems likely to present some interesting challenges for products, and also for ourselves. The results presented here should be taken as a rough guide only, and we expect to revamp the way we count detections for the next test, to take into account the likelihood of greyware items appearing in the Extended list. At the moment, our log processing systems discount grey alerts along with other suspicious calls, but for the initial runs at least we plan to count these as detections, in the Extended list only. We also plan to exclude non-*Windows* items, as many consumer solutions would not cover these with their standard default settings. There may be other changes required in the longer term, but we look forward to seeing how things go in the first run next time.

Of course, what many people are most interested in is how cloud connectivity will affect results, and we look forward to analysing that too. We have received some queries as to whether we will be comparing the results of products with and without their cloud lookups, to show how they might cope when cut off from their servers, and this is something we are looking into. We welcome any other suggestions, queries or criticisms (please email [john.hawes@virusbtn.com](mailto:john.hawes@virusbtn.com)), and as always aim to improve and expand our tests wherever we can.

#### Technical details

All products were tested on identical machines with *AMD Phenom II X2 550* processors, 4GB RAM, dual 80GB and 1TB hard drives, running *Microsoft Windows 2003 Server R2*, 32-bit Enterprise Edition, with Service Pack 2. For the full testing methodology please see <http://www.virusbtn.com/vb100/about/methodology.xml>.

*Any developers interested in submitting products for Virus Bulletin's VB100 comparative reviews should contact [john.hawes@virusbtn.com](mailto:john.hawes@virusbtn.com). The current schedule for the publication of VB100 comparative reviews can be found at <http://www.virusbtn.com/vb100/about/schedule.xml>.*

## VIRUS BULLETIN

**Editor:** Helen Martin

**Technical Editor:** Morton Swimmer

**Test Team Director:** John Hawes

**Anti-Spam Test Director:** Martijn Grooten

**Security Test Engineer:** Simon Bates

**Sales Executive:** Allison Sketchley

**Web Developer:** Paul Hettler

**Consulting Editors:**

Nick FitzGerald, *Independent consultant, NZ*

Ian Whalley, *IBM Research, USA*

Richard Ford, *Florida Institute of Technology, US*

## SUBSCRIPTION RATES

**Subscription price for Virus Bulletin magazine (including comparative reviews) for 1 year (12 issues):**

- Single user: \$175
- Corporate (turnover < \$10 million): \$500
- Corporate (turnover < \$100 million): \$1,000
- Corporate (turnover > \$100 million): \$2,000
- *Bona fide* charities and educational institutions: \$175
- Public libraries and government organizations: \$500

*Corporate rates include a licence for intranet publication.*

**Subscription price for Virus Bulletin comparative reviews only for 1 year (6 VBSpam and 6 VB100 reviews):**

- Comparative subscription: \$100

See <http://www.virusbtn.com/virusbulletin/subscriptions/> for subscription terms and conditions.

**Editorial enquiries, subscription enquiries, orders and payments:**

Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: [editorial@virusbtn.com](mailto:editorial@virusbtn.com) Web: <http://www.virusbtn.com/>

No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This publication has been registered with the Copyright Clearance Centre Ltd. Consent is given for copying of articles for personal or internal use, or for personal use of specific clients. The consent is given on the condition that the copier pays through the Centre the per-copy fee stated below.

VIRUS BULLETIN © 2011 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England. Tel: +44 (0)1235 555139. /2011/\$0.00+2.50. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.