JUNE 2011

virus BULLETIN Fighting malware and spam

JUNE 2011 VB100 COMPARATIVE REVIEW ON WINDOWS SERVER 2008 R2

INTRODUCTION

This month marks something of a departure for *VB*, as the regular VB100 comparative report is published separately from the monthly magazine issue for the first time. This will be the standard form of these reports in future, allowing more flexibility both for *VB* and for our readers. While *VB* subscribers will continue to have full access to both the monthly issues of *Virus Bulletin* and the comparative reports (as well as other benefits such as reduced conference rates), it is now possible to subscribe to the comparatives only – and for non-subscribers to purchase the reviews on an individual basis.

The change in format was not intended to impact the testing routine, with deadlines planned to remain much as they have in the past. This month has been something of an exception however, with a number of industry conferences at the start of May and some planned personal time later in the month making for a rather tight testing schedule – an issue exacerbated by illness in the lab team. As a result of this, and some other problems which will be described in more detail later, testing over-ran considerably; going forward, reports should be published closer to the middle of the month. A range of new tests we had hoped to include in this month's report have also had to be postponed, but we hope to include these very soon.

With the tight time frame known about in advance, we chose a server platform hoping for a somewhat smaller field of participants than in some of our recent desktop tests. When the deadline for submissions arrived, on 20 April, we were relatively pleased by the fairly slow pace of emails proffering products for us to test. At the final count just over 40 were included, which by recent standards is no more than a handful. A few newcomers bravely took the stand for their first appearance alongside most of our regular participants, and as always the mix of the new and the familiar promised an eventful month. After a blizzard of horrors in the recent *Windows XP* test, we entered the lab hoping to see stability and reliability from the products under test and, given the increased need for solidity and good behaviour in server environments, we intended to be more than usually severe in our criticism of any shortcomings.

PLATFORM AND TEST SETS

Our platform this month is *Windows Server 2008 R2*, the latest and shiniest server platform from *Microsoft*. Available for almost two years now, it corresponds to *Windows 7* much as the original *Server 2008* did to *Windows Vista*, and looks very similar in many respects to its desktop cousin. The installation process was complicated slightly by the demand for an extra partition at the start of the hard disk, which meant making some tweaks to our re-imaging set-up, but otherwise was uncomplicated and uneventful. We used the *Enterprise* version (although this should make little difference to how the products perform) and included no additional updates beyond the latest available service pack (the service pack was released in February and mainly comprises fixes for bugs and vulnerabilities with no major changes to the running of the platform). We added a few handy tools required for our tests, but set up no specific server 'roles', intending to add any additional software or settings as required by the products under test.

As usual, the test set deadline was set for a few days prior to the product submission date – 15 April in this case, and as such we missed the release of the March WildList by a few days (it emerged on the product submission deadline). Thus the February 2011 list was used for our core certification set, with few major surprises and no new instances of the complex polymorphic viruses that have created some excitement in recent tests. The clean sets – the other part of our core requirements – were updated considerably,

ISSN 1749-7027

including a wide selection of magazine cover CDs harvested in recent months. In addition, the usual range of software more common in business environments was added, this month including the addition of a selection of database packages and related data handling tools. With some pruning of older and less relevant items, the set remained roughly the same size, with some 450,000 unique files totalling around 250GB of data.

The other sets were compiled according to the usual processes. The RAP sets were built from samples harvested in the three weeks prior to the submission date and one week after, and the sets of trojans and other common malware put together from items first seen in the few weeks between the close of the last set of RAP tests and the start of the current one. The polymorphic set saw few changes, but we hope to update it considerably in the near future.

The speed sets were unchanged, containing the usual selection of common files from a range of systems at various levels of usage, categorized by file type to show how the products deal with different types of data. As in the last comparative, we also included on-demand scans and on-access runs over the system partition in our speed measures.

In order to keep testing time under control, we imposed a maximum limit of two hours on any individual scan in the on-demand speed tests – given that the majority of products need less than ten minutes to get through each of our standard speed sets, this seemed more than generous. As in previous tests, we hoped to get each product through the full suite of measures within a 24-hour period, which should be more than enough for most solutions. With the tests including scans of large volumes of malware, it would be inappropriate to penalize products too heavily for taking their time in some areas, so products are not denied certification if they over-run this limit, but we will mention any extravagant use of our limited lab time in the hope that vendors will sort out any issues.

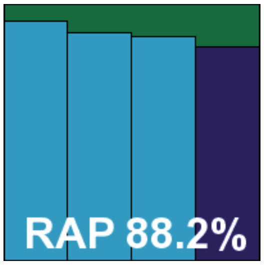
We also made some adjustments to our most recent addition, the set of standard activities. The sample sets were adjusted, reducing the quantity and size of the samples to allow us to increase the number of times the test is run, thus producing more accurate measures. As this was a server test, we expanded the selection of sample files – previously dominated by media such as videos, images and sounds files – to include items more likely to be found in corporate environments: *Microsoft Office* documents, presentations, PDF files and so on. Test scripts put these samples through a suite of common file manipulation tasks: first fetching them from a local web server via http, then copying, moving, compressing, decompressing, deleting and so on, to give a better idea of how the products under test impact everyday activities.

Agnitum Outpost Security Suite Pro

Version: 7.1 (3415.520.1248)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	91.35%
Worms & bots	95.26%	**False positives**	0

vb June 2011 100 VIRUS virusbtn.com



Agnitum's solution is aimed more at the consumer end of the market, but we always accept any product which can run happily on the test platform, and we expected several consumer-grade products in amongst the more server-oriented solutions this month. The installer came as a 111MB executable file including all required updates, and installed in a handful of standard stages. The only thing worth mentioning was the concealment of an option to join in with a community feedback scheme on the EULA page – most users would assume the checkbox indicated acceptance of the standard legal jargon and might well be surprised to learn they had given permission for information to be shared. The final stages of the set-up take some time, and a reboot is needed to complete.

The interface is clean and unfussy, following the standard approach to layout and providing a good level of usability. The company's main speciality is the firewall component, and unsurprisingly it is this area that gets most attention in the GUI design. However, a reasonable level of control is provided for the anti-malware portions, which are supported by the *VirusBuster* engine.

Running through the tests proved somewhat more time-consuming than we are used to with *Agnitum*'s solution, with sluggish scanning speeds and heavy overheads in the on-access measures. Memory consumption was not excessive but CPU use was fairly high, and impact on our suite of standard activities was also very heavy.

This sluggishness carried over to the infected sample sets; scanning our full sets on demand took quite some time, and while in previous tests we have seen some excellent optimization in the product – zipping through items already checked at lightning speeds – this feature was not in evidence on this platform, with on-access runs showing noticeably hefty overheads imposed by the product. As a result, testing took much longer than hoped, with almost a

On-demand tests	WildList		Worms & Bots		Polymorphic viruses		Trojans		Clean sets	
	Missed	%	Missed	%	Missed	%	Missed	%	FP	Susp.
Agnitum Outpost Security Suite Pro	0	100.00%	1369	95.26%	0	100.00%	4522	91.35%		
Arcabit ArcaVir 2011	0	100.00%	6977	75.86%	534	93.63%	13106	74.94%	1	
Avast Software avast! 4.8	0	100.00%	492	98.30%	2	99.98%	4051	92.25%		
Avertive VirusTect	0	100.00%	1665	94.24%	0	100.00%	7046	86.53%		
AVG Internet Security 2011	0	100.00%	373	98.71%	4	99.99%	1292	97.53%		
Avira AntiVir Server	0	100.00%	86	99.70%	0	100.00%	542	98.96%		
BitDefender Security for File Servers	0	100.00%	68	99.76%	0	100.00%	586	98.88%		
Bkis BKAV Professional I.S.	0	100.00%	53	99.82%	0	100.00%	117	99.78%		
Bullguard AntiVirus	0	100.00%	65	99.78%	0	100.00%	521	99.00%		
CA Total Defense r12 I.S.	0	100.00%	2377	91.78%	4	99.96%	10676	79.59%		
Central Command Vexira	0	100.00%	1449	94.99%	0	100.00%	5887	88.74%		
Clearsight Antivirus	0	100.00%	1665	94.24%	0	100.00%	7046	86.53%		
Commtouch Command Anti-Malware	0	100.00%	4622	84.01%	0	100.00%	11044	78.88%	2	2
Coranti 2010	0	100.00%	26	99.91%	0	100.00%	148	99.72%	2	2
Defenx Security Suite 2011	0	100.00%	1348	95.34%	0	100.00%	4507	91.38%		
Digital Defender	0	100.00%	1665	94.24%	0	100.00%	7046	86.53%		
eEye Blink Server	0	100.00%	1065	96.32%	4	99.98%	2097	95.99%		1
Emsisoft Anti-Malware for Server	0	100.00%	105	99.64%	432	95.61%	435	99.17%	1	
eScan Internet Security Suite	0	100.00%	68	99.76%	0	100.00%	541	98.97%		
ESET NOD32 Antivirus	0	100.00%	1055	96.35%	3	99.99%	2939	94.38%		14
Fortinet FortiClient	0	100.00%	842	97.09%	0	100.00%	3262	93.76%		
Frisk F-PROT Antivirus	0	100.00%	5096	82.37%	0	100.00%	11932	77.19%	2	
F-Secure Protection Service	0	100.00%	66	99.77%	0	100.00%	457	99.13%		
G Data AntiVirus Client	0	100.00%	8	99.97%	0	100.00%	119	99.77%	1	
Ikarus virus.utilities	0	100.00%	163	99.44%	432	95.61%	489	99.07%	1	
Kaspersky Small Office Security	0	100.00%	320	98.89%	0	100.00%	2473	95.27%		
Keniu Antivirus	0	100.00%	304	98.95%	0	100.00%	12293	76.50%	1	
Kingsoft AntiVirus 2011 Advanced A	0	100.00%	15821	45.27%	407	96.04%	34678	33.70%		
Kingsoft AntiVirus 2011 Advanced B	0	100.00%	11707	59.50%	493	95.89%	20363	61.07%	7	
Kingsoft AntiVirus 2011 Standard	0	100.00%	18300	36.70%	418	96.03%	42184	19.34%		
Lumension EMSS	0	100.00%	958	96.69%	4	99.98%	1878	96.41%		1
Microsoft Forefront Endpoint Protection 2010	0	100.00%	618	97.86%	0	100.00%	4773	90.87%		
Mongoosa	0	100.00%	1661	94.25%	0	100.00%	5581	89.33%		
Norman Security Suite	0	100.00%	1060	96.33%	4	99.98%	2059	96.06%		1
Preventon Antivirus for Server	0	100.00%	1665	94.24%	0	100.00%	7046	86.53%		
Quick Heal AntiVirus 2011 Server Ed.	0	100.00%	737	97.45%	0	100.00%	1848	96.47%		
Returnil System Safe 2011	0	100.00%	4623	84.01%	0	100.00%	11044	78.88%	2	1
Sophos Endpoint Security and Control	0	100.00%	924	96.80%	0	100.00%	6313	87.93%		1
SPAMfighter VIRUSfighter	0	100.00%	1665	94.24%	0	100.00%	7046	86.53%		
GFI/Sunbelt VIPRE Antivirus	0	100.00%	386	98.66%	19	99.79%	1668	96.81%		
TGSoft VirIT eXplorer PRO	764	62.88%	15470	46.49%	12986	63.76%	39051	25.33%	4	
Trustport Antivirus 2011	0	100.00%	4	99.99%	0	100.00%	137	99.74%		
VirusBuster For Windows Server	0	100.00%	6007	79.22%	0	100.00%	4528	91.34%		

(Please refer to text for full product names.)

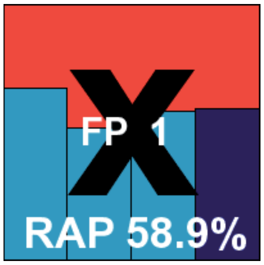
full working week needed to get through the full suite of measures.

When eventually everything was completed to our satisfaction, the scores were fairly decent, with good coverage in the standard sets and respectable scores across the four weeks of the RAP sets. The WildList caused no problems, and with the clean sets handled well too, *Agnitum* earns a VB100 award and continues its run of good showings in the VB100 certification system; the vendor has five passes in the last six tests (having only skipped the annual *Linux* test earlier this year), and seven passes from eight entries in the last two years.

Arcabit ArcaVir 2011

Version 11.4.6403.1

ItW	100.00%	**Polymorphic**	93.63%
ItW (o/a)	100.00%	**Trojans**	74.94%
Worms & bots	75.86%	**False positives**	1



Arcabit's product was provided as a fairly large 182MB install package, including latest updates, and took quite some time to get set up. There were not too many stages to go through, but there were several rather long and worryingly silent pauses while various bits were put in place. No reboot was needed at the end however.

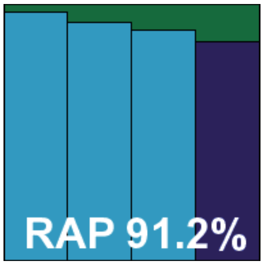
The interface uses the large button approach, with no main menu down the side, but is fairly intuitive to use and provides a good level of configuration. Stability seemed much improved, continuing a trend observed over several comparatives, and there were no problems completing the test suite. Scanning speeds were pretty fast, especially considering the completeness of coverage – including most archive types by default – while on-access lags were perhaps just a fraction on the high side in some areas, but without any serious spikes. Memory use was not too high, and CPU use was reasonable too. Impact on our set of activities was minimal.

Detection rates were rather mediocre in most areas, rather unpredictable in the RAP sets, but the WildList was handled without problems. In the clean set however, a single item was alerted on, which was enough to deny *Arcabit* a VB100 award once again. This continuation of a run of bad luck gives *Arcabit* four fails out of four entries in the past year, with only one pass from six attempts in the last dozen tests.

Avast Software avast! 4.8

Build: Sep 2009 (4.8.1114), VPS file version: 110420-1

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	92.25%
Worms & bots	98.30%	**False positives**	0



Avast submitted its mature 4.8 version for this month's test, promising a new server edition to complement the shiny new desktop product soon. The product was provided as a compact 66MB executable, including all updates, and installed simply and logically, with a slight old-school tone to the dialogs. A reboot was needed to complete the set-up.

The interface is starting to look a little old and creaky, especially compared to the latest glitzy products, but is solid and well designed, offering excellent configuration options (particularly in the default 'advanced' mode), and it operated smoothly throughout the tests.

Speeds were as zippy as ever, powering through all our tests with barely a flicker or hesitation, and everything was out of the way in well under the allotted 24 hours. Scanning speeds were super-fast, and on-access overheads not too heavy, with light use of resources but a noticeable effect on our suite of tasks.

Detection rates were very solid indeed, with only a gentle downturn in the latter parts of the RAP sets; the WildList and clean sets presented no difficulties, and a VB100 award is easily earned. *Avast* has an impeccable record in our tests of late, having neither missed a test nor failed to pass since the end of 2008.

Avertive VirusTect

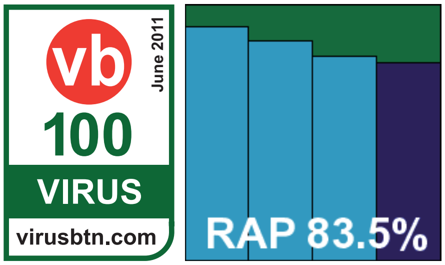
Version: 1.1.56, Definitions date: 18/04/2011, Definitions version: 13.6.311

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.53%
Worms & bots	94.24%	**False positives**	0

The first of the usual cluster of products based on the *Preventon* SDK and the *VirusBuster* engine, this month *Avertive* requested installation with an Internet connection

On-access tests	WildList		Worms & bots		Polymorphic viruses		Trojans	
	Missed	%	Missed	%	Missed	%	Missed	%
Agnitum Outpost Security Suite Pro	0	100.00%	1485	94.86%	0	100.00%	6915	86.78%
Arcabit ArcaVir 2011	0	100.00%	7019	75.72%	534	93.63%	13112	74.93%
Avast Software avast! 4.8	0	100.00%	181	99.37%	2	99.98%	1312	97.49%
Avertive VirusTect	0	100.00%	1682	94.18%	0	100.00%	7046	86.53%
AVG Internet Security 2011	0	100.00%	389	98.65%	4	99.99%	1774	96.61%
Avira AntiVir Server	0	100.00%	182	99.37%	0	100.00%	798	98.47%
BitDefender Security for File Servers	0	100.00%	67	99.77%	0	100.00%	501	99.04%
Bkis BKAV Professional I.S.	0	100.00%	56	99.81%	0	100.00%	625	98.80%
Bullguard AntiVirus	0	100.00%	67	99.77%	0	100.00%	538	98.97%
CA Total Defense r12 I.S.	0	100.00%	2377	91.78%	4	99.96%	10676	79.59%
Central Command Vexira	0	100.00%	1739	93.98%	0	100.00%	6993	86.63%
Clearsight Antivirus	0	100.00%	1682	94.18%	0	100.00%	7047	86.53%
Commtouch Command Anti-Malware	0	100.00%	5095	82.38%	0	100.00%	11951	77.15%
Coranti 2010	0	100.00%	135	99.53%	0	100.00%	1812	96.54%
Defenx Security Suite 2011	0	100.00%	1485	94.86%	0	100.00%	6915	86.78%
Digital Defender	0	100.00%	1682	94.18%	0	49.35%	17396	66.74%
eEye Blink Server	0	100.00%	1185	95.90%	38	99.66%	2842	94.57%
Emsisoft Anti-Malware for Server	0	100.00%	162	99.44%	432	95.61%	489	99.07%
eScan Internet Security Suite	0	100.00%	241	99.17%	0	100.00%	2682	94.87%
ESET NOD32 Antivirus	0	100.00%	1232	95.74%	0	100.00%	5408	89.66%
Fortinet FortiClient	0	100.00%	840	97.09%	0	100.00%	3261	93.76%
Frisk F-PROT Antivirus	0	100.00%	5232	81.90%	0	100.00%	13997	73.24%
F-Secure Protection Service	0	100.00%	161	99.44%	0	100.00%	2466	95.28%
G Data AntiVirus Client	0	100.00%	103	99.64%	0	100.00%	385	99.26%
Ikarus virus.utilities	0	100.00%	163	99.44%	432	95.61%	489	99.07%
Kaspersky Small Office Security	0	100.00%	431	98.51%	0	100.00%	2732	94.78%
Keniu Antivirus	0	100.00%	4112	85.78%	0	100.00%	15809	69.77%
Kingsoft AntiVirus 2011 Advanced A	0	100.00%	15838	45.21%	407	96.04%	34810	33.44%
Kingsoft AntiVirus 2011 Advanced B	0	100.00%	11820	59.11%	493	95.89%	20598	60.62%
Kingsoft AntiVirus 2011 Standard	0	100.00%	18316	36.64%	418	96.03%	42327	19.07%
Lumension EMSS	0	100.00%	1079	96.27%	38	99.66%	2568	95.09%
Microsoft Forefront Endpoint Protection 2010	0	100.00%	813	97.19%	0	100.00%	5579	89.33%
Mongoosa	0	100.00%	1808	93.75%	0	100.00%	7912	84.87%
Norman Security Suite	0	100.00%	1183	95.91%	38	99.66%	2842	94.57%
Preventon Antivirus for Server	0	100.00%	1682	94.18%	0	100.00%	7047	86.53%
Quick Heal AntiVirus 2011 Server Ed.	0	100.00%	3300	88.58%	0	100.00%	7188	86.26%
Returnil System Safe 2011	0	100.00%	5278	81.74%	0	100.00%	13991	73.25%
Sophos Endpoint Security and Control	0	100.00%	820	97.16%	0	100.00%	3702	92.92%
SPAMfighter VIRUSfighter	0	100.00%	1700	94.12%	0	100.00%	7054	86.51%
GFI/Sunbelt VIPRE Antivirus	0	100.00%	722	97.50%	40	99.50%	1032	98.03%
TGSoft VirIT eXplorer PRO	3714	62.52%	15545	46.23%	25531	37.85%	39228	25.00%
Trustport Antivirus 2011	0	100.00%	82	99.72%	0	100.00%	493	99.06%
VirusBuster For Windows Server	0	100.00%	1739	93.98%	0	100.00%	6993	86.63%

(Please refer to text for full product names.)



to fetch latest updates, rather than bundling them with the install package as in previous tests. The 73MB installer took 30 seconds or so orienting itself before presenting its welcome screen, and ran through a simple, standard process to get things in place, with no need for a restart. On connecting to the web, a licence key is checked against the server before full access is granted to the configuration controls. The update ran fairly quickly, although rather oddly it reported a date two days prior to that on which the update was run.

Once up and running, the interface is very simple and easy to operate, providing only basic controls. One serious issue we faced was with the logging system, which by default abandons all data after reaching certain caps (around 4MB for on-access results and 20MB for on-demand scans). As the default setting is very verbose, recording a verdict on every file inspected, it would be very easy to run a large scan of a normal system which failed to record full details of all items found in the logs. An option is provided to log only the points of interest, but to increase the cap some doctoring of registry entries is required.

This was not too arduous though, and running through the speed tests proved reasonably speedy and reliable. On-demand speeds were good, and overheads fairly light, with RAM and CPU use well within normal bounds and impact on our set of tasks barely noticeable. Detection tests were not the fastest, but nevertheless all our work was completed in reasonable time.

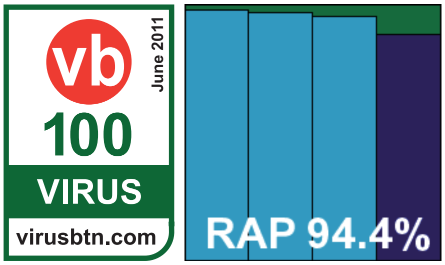
Scores were respectable if not stellar, with a steady decline across the weeks of the RAP sets from a decent starting point. The WildList and clean sets were dealt with successfully, and a VB100 award is duly earned. In less than a year of entries, *Avertive* now has two passes and two fails, with one test skipped.

AVG Internet Security Business Edition 2011

AVG version: 10.0.1321, Virus DB: 1500/3583

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	97.53%
Worms & bots	98.71%	**False positives**	0

AVG's business product was provided as a fairly sizeable 179MB installer, including updates, and ran through some standard steps, including the offer of a security browser toolbar, taking some time to unpack everything but completing in reasonable time with no need to restart.



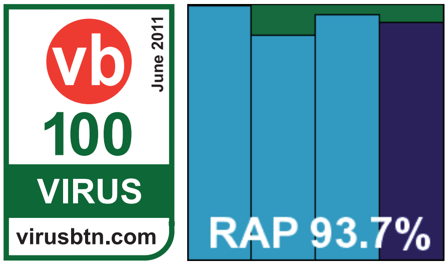
The interface looks fairly similar to the company's consumer range, but in a more sober, grey colour scheme. The layout uses a standard approach, making it simple to operate, and provides excellent controls. Scanning speeds were decent from the off and sped up hugely on repeat visits, and on-access overheads were feather-light. Memory use was higher than some, but processor use was low and impact on our set of activities was minimal.

Detection tests ran through in good time without problems, and showed excellent detection rates across the board, dipping slightly in the proactive week of the RAP sets. The WildList and clean sets presented no difficulties, and a VB100 award is comfortably earned. *AVG*'s streak of VB100 successes runs back to the summer of 2007, but skipping the 2010 *Linux* test means the company has 11 passes from the last 12 tests.

Avira AntiVir Server

Product version 10.0.0.1807, Virus definition file 7.11.06.179

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.96%
Worms & bots	99.70%	**False positives**	0

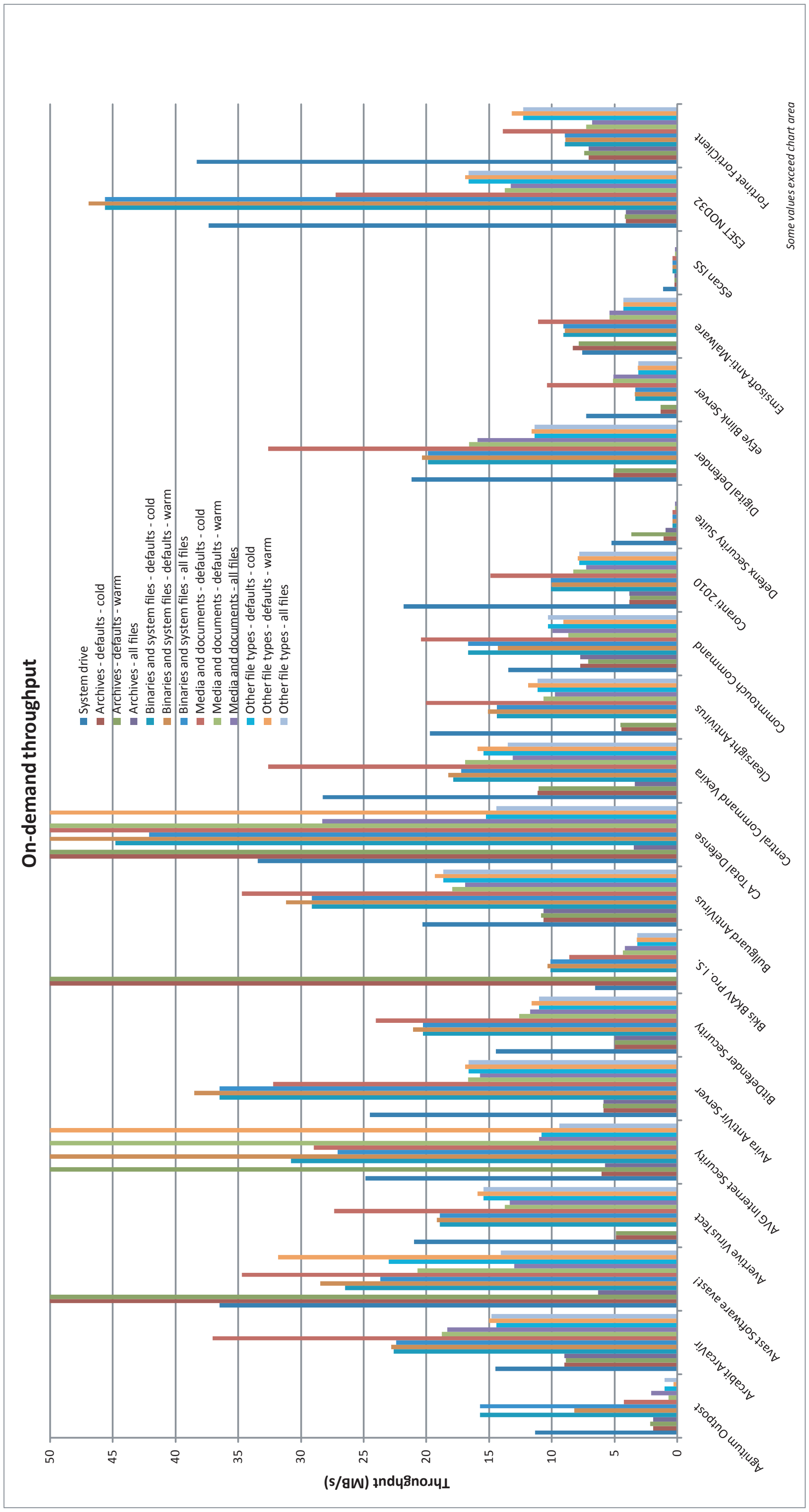


Avira submitted a fully server-oriented solution this month, which came as a compact 57MB package including updates. The install process is simple and rapid, with most of the time taken up putting C++ components in place. With no need for a reboot we are led straight into a configuration wizard. This sensibly offers to exclude common server

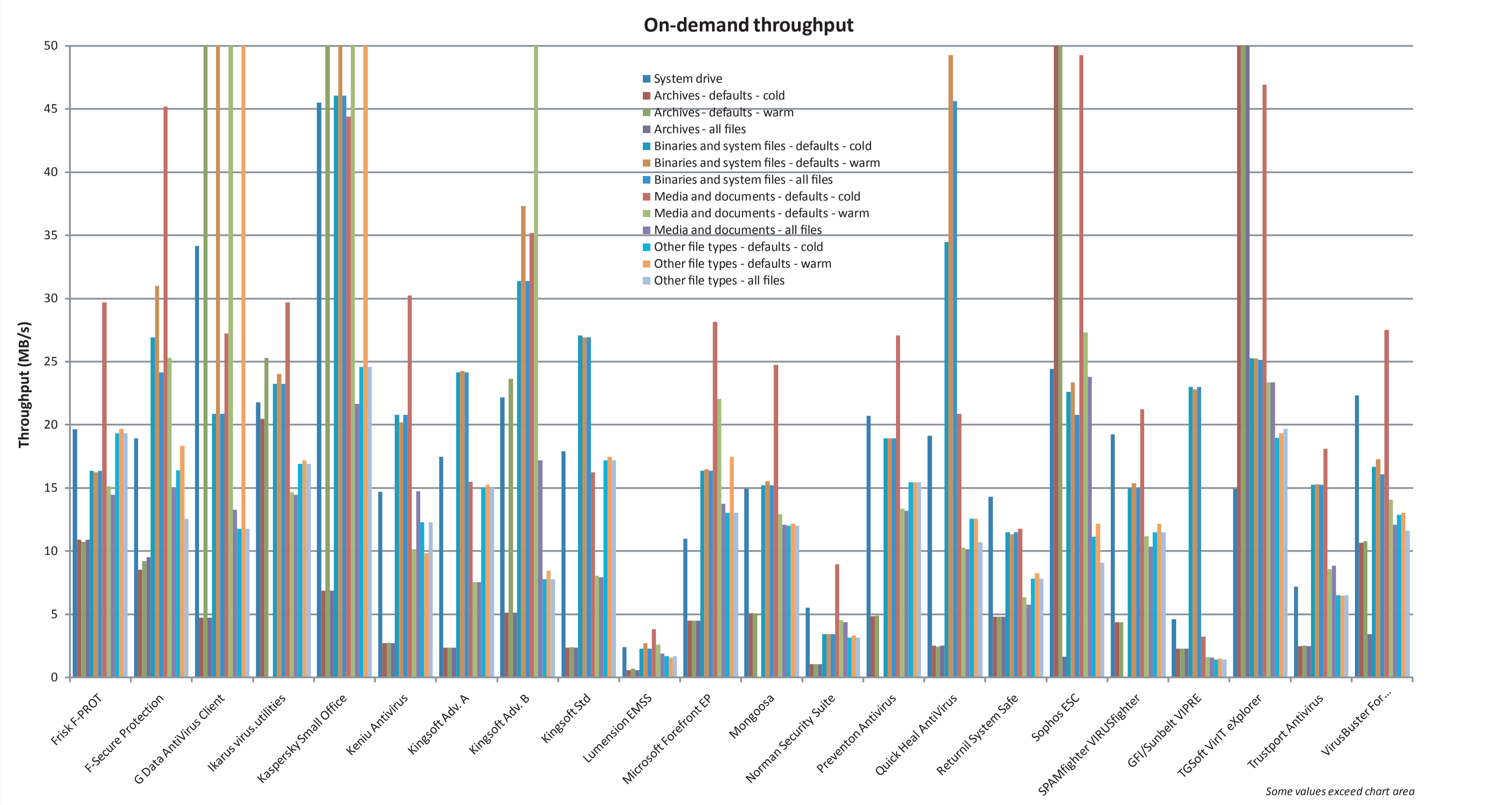
On-demand throughput (MB/s)	System drive*	Archive files			Binaries & system files			Media & documents			Other file types		
		Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files	Default (Cold)	Default (Warm)	All files
Agnitum Outpost	11.36	1.95	2.18	1.95	15.74	8.24	15.74	4.27	0.72	2.09	1.02	0.33	1.02
Arcabit ArcaVir	14.50	9.03	8.89	9.03	22.60	22.81	22.39	37.04	18.79	18.35	14.43	15.03	14.82
Avast Software avast!	36.47	116.28	126.39	6.32	26.48	28.47	23.68	34.69	20.73	13.00	23.02	31.82	14.05
Avertive VirusTect	20.99	4.92	4.92	NA	18.95	19.17	18.95	27.37	13.74	13.36	15.46	15.91	15.46
AVG Internet Security	24.87	6.03	2906.94	5.78	30.79	1642.04	27.07	28.98	400.75	11.03	10.82	270.50	9.41
Avira AntiVir Server	24.51	5.91	5.92	5.91	36.49	38.49	36.49	32.20	16.70	15.72	16.65	16.91	16.65
BitDefender Security	14.49	4.98	4.99	4.98	20.27	21.05	20.27	24.03	12.59	11.73	11.04	11.63	11.04
Bkis BKAV Professional	6.57	88.09	96.90	NA	10.12	10.35	10.12	8.61	4.33	4.20	3.20	3.24	3.20
Bullguard AntiVirus	20.33	10.69	10.89	10.69	29.15	31.18	29.15	34.69	17.94	16.93	18.66	19.32	18.66
CA Total Defense	33.42	145.35	2906.94	3.47	44.78	1642.04	42.10	62.36	343.50	28.29	15.24	270.50	14.43
Central Command Vexira	28.28	11.14	11.05	3.39	17.85	18.24	17.22	32.62	16.93	13.14	15.46	15.91	13.53
Clearsight Antivirus	19.71	4.48	4.54	NA	14.40	15.11	14.40	20.02	10.69	9.77	11.15	11.89	11.15
Commtouch Command	13.47	7.73	7.12	7.73	16.70	14.32	16.70	20.44	8.68	9.98	10.30	9.09	10.30
Coranti 2010	21.83	3.85	3.79	3.85	10.09	9.99	10.09	14.88	8.32	7.26	7.84	7.96	7.84
Defenx Security Suite	5.25	1.10	3.66	0.95	0.41	0.41	0.41	0.41	0.20	0.20	0.09	0.09	0.09
Digital Defender	21.19	5.08	5.08	NA	19.86	20.36	19.86	32.62	16.58	15.92	11.39	11.63	11.39
eEye Blink Server	7.25	1.34	1.34	NA	3.35	3.39	3.35	10.41	5.13	5.08	3.11	3.17	3.11
Emsisoft Anti-Malware	7.61	8.33	7.86	NA	9.09	8.99	9.09	11.12	5.42	5.43	4.33	4.33	4.33
eScan ISS	1.13	0.24	0.24	0.24	0.41	0.41	0.41	0.41	0.20	0.20	0.09	0.09	0.09
ESET NOD32	37.37	4.11	4.21	4.11	45.61	46.92	45.61	27.22	13.74	13.28	16.65	16.91	16.65
Fortinet FortiClient	38.32	7.06	7.43	7.06	8.97	8.94	8.97	13.92	7.26	6.79	12.30	13.20	12.30
Frisk F-PROT	19.63	10.93	10.77	10.93	16.37	16.26	16.37	29.68	15.12	14.48	19.32	19.67	19.32
F-Secure PS	18.94	8.52	9.23	9.53	26.92	30.98	24.15	45.19	25.31	14.93	16.39	18.34	12.58
G Data AntiVirus Client	34.16	4.73	2906.94	4.73	20.87	1642.04	20.87	27.22	480.90	13.28	11.76	541.00	11.76
Ikarus virus.utilities	21.80	20.47	25.28	NA	23.24	24.03	23.24	29.68	14.66	14.48	16.91	17.17	16.91
Kaspersky Small Office	45.49	6.87	2906.94	6.87	46.04	547.35	46.04	44.38	92.48	21.66	24.59	98.36	24.59
Keniu Antivirus	14.72	2.74	2.76	2.74	20.79	20.19	20.79	30.22	10.15	14.75	12.30	9.84	12.30
Kingsoft AntiVirus Adv. A	17.46	2.37	2.38	2.37	24.15	24.27	24.15	15.49	7.56	7.56	15.03	15.24	15.03
Kingsoft AntiVirus Adv. B	22.19	5.15	23.63	5.15	31.38	37.32	31.38	35.19	100.19	17.18	7.78	8.45	7.78
Kingsoft AntiVirus Std.	17.90	2.38	2.40	2.38	27.07	26.92	26.92	16.26	8.07	7.94	17.17	17.45	17.17
Lumension EMSS	2.40	0.61	0.70	0.61	2.28	2.73	2.28	3.85	2.62	1.88	1.71	1.58	1.71
Microsoft Forefront	10.98	4.50	4.49	4.50	16.37	16.48	16.37	28.15	22.06	13.74	13.04	17.45	13.04
Mongoosa	14.95	5.12	5.10	NA	15.20	15.54	15.20	24.75	12.93	12.08	12.02	12.16	12.02
Norman Security Suite	5.54	1.08	1.08	1.08	3.43	3.46	3.43	8.99	4.55	4.39	3.17	3.32	3.17
Preventon Antivirus	20.70	4.88	4.90	NA	18.95	18.95	18.95	27.07	13.36	13.21	15.46	15.46	15.46
Quick Heal AntiVirus	19.13	2.54	2.47	2.51	34.45	49.26	45.61	20.87	10.28	10.15	12.58	12.58	10.71
Returnil System Safe	14.30	4.81	4.83	4.81	11.51	11.32	11.51	11.78	6.36	5.75	7.84	8.26	7.84
Sophos ESC	24.42	223.61	264.27	1.65	22.60	23.35	20.79	49.26	27.32	23.81	11.15	12.16	9.09
SPAMfighter VIRUSfighter	19.27	4.40	4.39	NA	14.97	15.39	14.97	21.23	11.18	10.36	11.51	12.16	11.51
GFI/Sunbelt VIPRE	4.63	2.30	2.30	2.30	23.02	22.81	23.02	3.26	1.63	1.59	1.41	1.50	1.41
TGSoft VirIT eXplorer	14.93	322.99	290.69	161.50	25.26	25.26	25.13	46.92	23.34	23.34	18.98	19.32	19.67
Trustport Antivirus	7.19	2.48	2.53	2.48	15.25	15.30	15.25	18.11	8.59	8.84	6.52	6.48	6.52
VirusBuster	22.33	10.69	10.81	3.45	16.70	17.28	16.10	27.52	14.06	12.08	12.88	13.04	11.63

* System drive measure shows the average throughput of two scans of the system (C:) partition using default settings – one 'cold' and one 'warm' run.

(Please refer to text for full product names.)



(Please refer to text for full product names.)



(Please refer to text for full product names.)

components (such as databases) from scanning, with a list of likely candidates provided.

The interface uses the Microsoft Management Console (MMC), which some products in the past have made something of a meal of. However, in this case it is clear and rationally laid out with all options easy to find and operate. The term ‘a joy to use’ was even uttered by one member of the lab team.

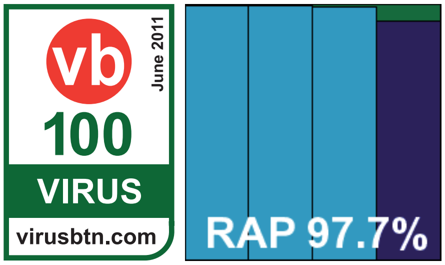
Scanning speeds were excellent, with light overheads on access, and use of memory and CPU were both on the low side, while our set of activities ran through only slightly slower than on unprotected systems.

Detection rates were superb as usual, with most of the sets covered excellently, and the WildList and clean sets were no exception, earning *Avira* another VB100 award. *Avira*’s test history shows a solid record of six passes out of six entries in the last year, and 11 out of the last 12 tests passed.

BitDefender Security for File Servers

Version 3.5 (3.5.16.21/3.5.16.42)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.88%
Worms & bots	99.76%	**False positives**	0



Another fully fledged server solution, *BitDefender*’s installer is a little larger at 179MB, and again includes all the necessary updates. The install process has no more than the usual number of steps to work through but runs a little on the slow side, with no need to reboot at the end. Another set-up wizard is provided after the main work is done.

The interface again uses the MMC system, introducing rather more colour and glitz than most, but remaining clear and easy to use. One minor issue noted was that it took rather a long time to save logs after some scans, but this is only likely to occur when large numbers of detections are involved, which is unlikely in the real world.

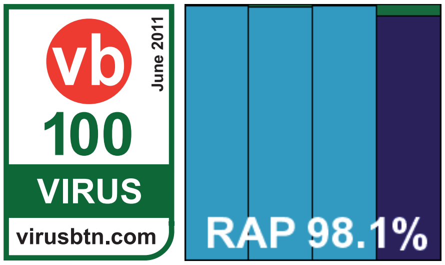
Scanning speeds were reasonable, with no sign of the optimization we have seen in some other products from the same vendor. On access, overheads were fairly light, but CPU use was fairly high, with RAM around average. Impact on our set of tasks was perhaps a fraction higher than most, but not excessively so.

Detection rates were extremely high, with very little missed anywhere, including a superb showing in the RAP sets. The core certification requirements were met with ease, and *BitDefender* earns another VB100 award, its fifth pass in the last year. The vendor’s two-year history shows nine passes from 12 tests, with two tests not entered and only a single fail.

Bkis BKAV Professional Internet Security

Definition version: 3286, Engine version: 3.6.6, Pattern codes: 7.694.190

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.78%
Worms & bots	99.82%	**False positives**	0



This month’s submission from *Bkis* was fairly large at 212MB including updates, but powered through the install process in just a couple of clicks and perhaps 10 seconds of waiting. A reboot was required to complete the process. The interface is a rather gaudy orange colour, but is simple and easy to use, although it provides only very minimal configuration controls.

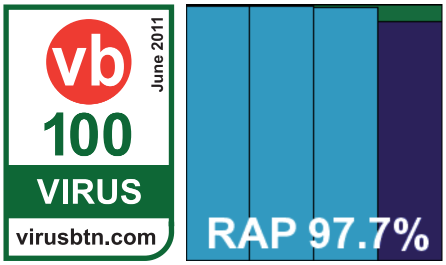
Scanning speeds were not super-fast, except in the archive sets where archives were not scanned internally, and on-access overheads were fairly heavy. CPU and RAM use were a little high too, and impact on our suite of activities was certainly noticeable.

Detection rates were excellent though, with very high scores across the board once again. The WildList was easily covered, and with no repeat of the false positive issue encountered in the last test, *Bkis* earns another VB100 award. This version of the *Bkis* product has a decent record, having passed four of the last six tests, with one fail and a single (*Linux*) test not entered.

Bullguard AntiVirus 10

Version 10.0.179

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.00%
Worms & bots	99.78%	**False positives**	0



Bullguard's product came as a 150MB installer, fully updated. It installed in only a few quick steps with no need to reboot. The interface is bright and colourful, with a slightly quirky approach which soon becomes simple to navigate after some initial exploring.

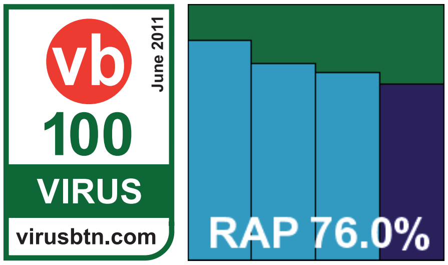
Testing proved fairly painless, with very fast scanning times and fairly light overheads, although memory use was a little high and our set of tasks ran a little slowly. There were no stability problems, and all tests were completed in good time.

Detection rates were uniformly excellent, with stunning coverage of the RAP sets, and the core certification sets were handled admirably too. *Bullguard* thus comfortably earns a VB100 award, its history showing only sporadic entries but solid pass rates, with three passes from three entries in the last year, five from five entries in the last dozen tests.

CA Total Defense r12 Internet Security

Version 12.0.528, Client agent 12.0.0.621, Anti-malware engine 1.3.3.1269, Anti-malware signatures 4296.0.0.0

ItW	100.00%	**Polymorphic**	99.96%
ItW (o/a)	100.00%	**Trojans**	79.59%
Worms & bots	91.78%	**False positives**	0



CA's revamped enterprise product has given us a few headaches in the past, but with some familiarity things are becoming easier. Although the specs indicated that the management system supported the test platform, the installer refused to run – possibly baffled by the relatively recent service pack. Fortunately, we were able to dig up an older install on *Windows 7*, and although once again we had no luck deploying it directly across the network, it was not too challenging to create a standalone install bundle and copy it across to the final test system. The install process was fairly fast and simple from there, with a reboot required to complete. After the reboot, the test machine became unresponsive for some time, with the screen going blank after the initial desktop preparation stage, but the traditional three-key approach soon got it back on its feet. Updates were run online on the deadline day, taking almost an hour and a half to apply the necessary 500MB of data.

The interface is pleasantly designed – clear and friendly without too much fussiness. A reasonable level of controls are available, although by default the client level has little access to these – quite sensibly, policy tweaks are required to allow end-users much control over their protection systems.

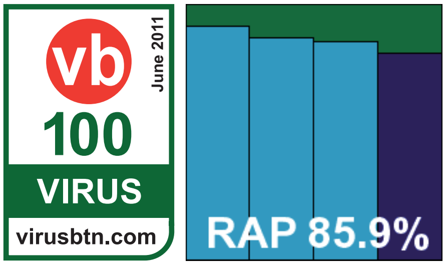
Performance tests ran through without too much difficulty, the speed measures showing the usual very rapid scanning and light file access lag times, although use of both RAM and CPU was fairly high. Our suite of tasks ran through in good order with little additional time taken.

Scanning our infected sets once again proved a pain, with storage of large amounts of data in memory leading to some rather depressing slowdowns. Running large numbers of smaller scans with frequent reboots in between helped to an extent, but still several days were needed to get everything done. Detection levels were respectable if not exactly stellar, with a steady decrease through the RAP sets. The WildList and clean sets were well handled though, and a VB100 award is duly earned. *CA*'s corporate product line now has three passes and two fails in the last year, with one test not entered, seven passes and three fails in the last 12 comparatives.

Central Command Vexira Antivirus for Windows Servers

Product version 7.1.52, Scan engine 5.2.0, Virus database 13.6.13 (20/04/2011)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	88.74%
Worms & bots	94.99%	**False positives**	0



Vexira has re-emerged of late to become a dependable member of our growing list of regulars on the VB100 test bench. The server version provided this month came as a 65MB installer with

68MB of updates, The set-up process was clear and simple, taking a minute or so to go through the standard stages and requesting a reboot at the end.

The interface is another that uses the MMC system, and is a little awkward in places, lacking intuitiveness and consistency from one section to another, but with some practice it was reasonably tractable. The scheduler proved beyond us however, and several jobs which we thought were properly prepared failed to run for some reason.

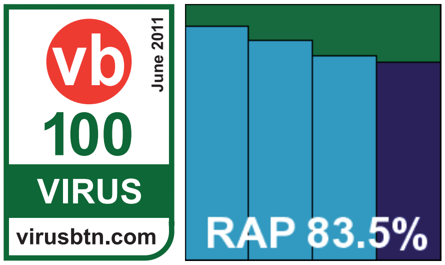
Nevertheless, we got through the test suite in good time, with none of the extreme slowdowns noted in the last comparative. Scanning speeds were pretty fast, and lag times fairly low, with minimal RAM and CPU drain but a fairly heavy impact on our set of activities.

Detection rates were decent, not dropping too sharply in the RAP sets, and there were no problems in the WildList or clean sets, earning *Central Command* another VB100 award. In the eight tests entered since the product was revamped, *Vexira* boasts a flawless record of passes.

Clearsight Antivirus

Version: 1.1.56, Definitions date: 18/04/2011, Definitions version: 13.6.311

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.53%
Worms & bots	94.24%	**False positives**	0



As with other products from the same family, *Clearsight* requested online updates, and after running the fast and simple 74MB install package (which needs no reboot to complete), updating ran rapidly without too much fuss – but once again reported a date a few days old.

The interface is very familiar by now, remaining simple and easy to use and providing a basic level of controls. *Clearsight* differs from its fellows in having a crisp blue-and-white colour scheme.

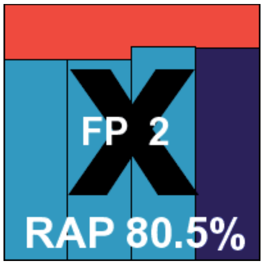
Speed measures were dependably decent, with fairly good scanning speeds and fairly light lag times on access, low use of resources and little impact on our set of tasks.

Running through the infected sets was noticeably slower than usual, with the on-access component shutting down unexpectedly during one run, but a second try got it through without too much difficulty. Detection rates were also decent, with good levels over older samples and a slight decrease into the later weeks of the RAP sets. The core certification sets caused no problems though, and *Clearsight* earns a VB100 award without too much fuss. A relative newcomer to our tests, *Clearsight* now has two passes from the last four tests, two of which were not entered.

Commtouch Command Anti-Malware

Product version: 5.1.12, Engine version: 5.3.2, Dat file ID: 201104200836

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	78.88%
Worms & bots	84.01%	**False positives**	2



Another fairly dependable regular in our tests these days, *Commtouch*'s product comes as a tiny 13MB installer with 45MB or so of updates provided separately. The set-up process is fast and simple, including an option to detect 'potentially unwanted' items, and the GUI is pared-down in the extreme, with very simple controls providing basic configuration, and everything in easy reach.

Scanning speeds were not too fast and on-access lag times a little heavy. CPU use and impact on our set of activities were decidedly high. One scan through our full sets seemed to give up halfway through, but a rerun managed to complete without problems and we still managed to get through the tests in reasonable time.

Detection rates were a little below par, but still fairly respectable, and the WildList was handled without problems. In the clean sets, however, a couple of items were labelled malicious, including a version of the hugely prevalent *iTunes* application, and *Commtouch* is thus denied a VB100 award this month. Having a rather rocky time of late, *Command* has a history of two passes, two fails and two no-entries from the last year, with three passes, four fails and five no-entries in the last 12 tests.

Coranti 2010

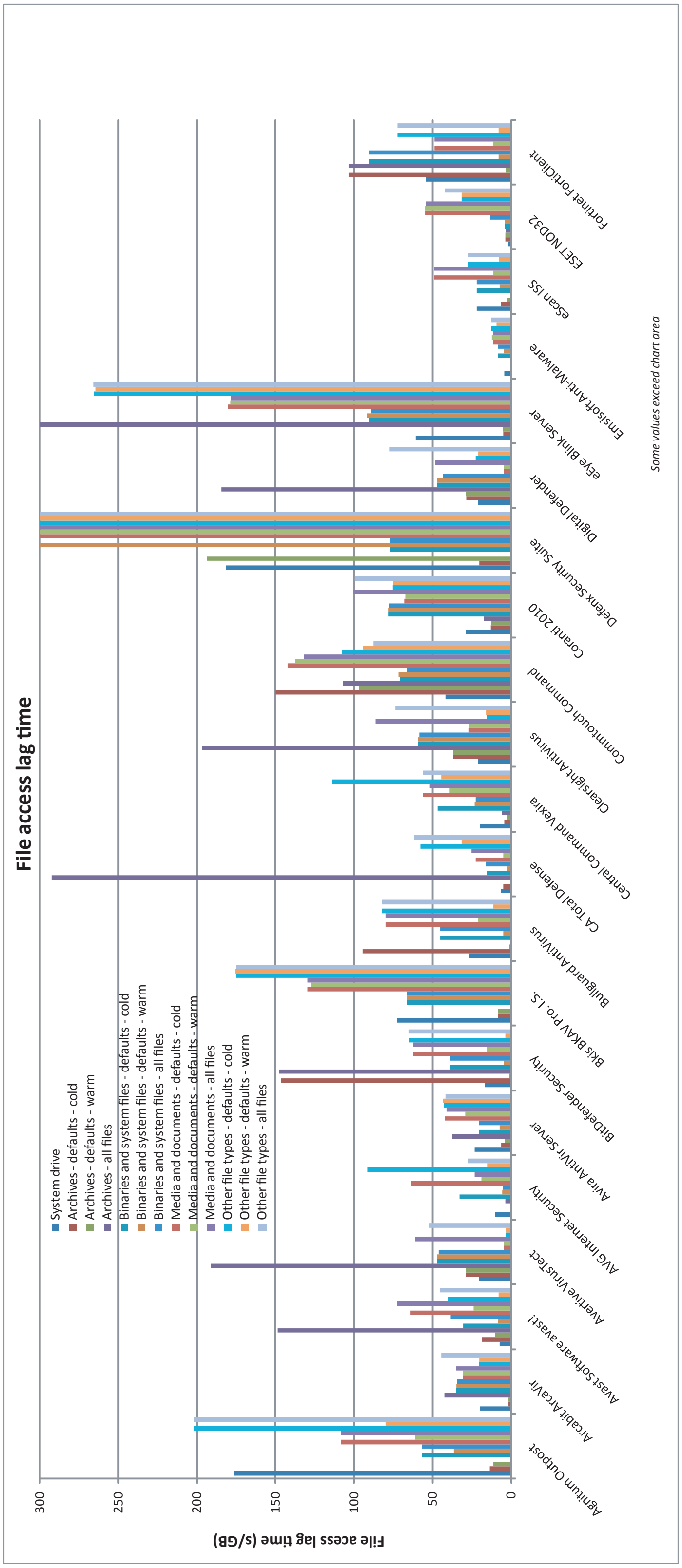
Product version 1.003.00001, Definitions database v. 6301

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.72%
Worms & bots	99.91%	**False positives**	2

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	176.53	13.69	11.45	NA	56.88	36.60	56.88	108.30	61.16	108.30	201.96	79.90	201.96
Arcabit ArcaVir	20.03	1.71	1.74	42.52	35.05	34.90	34.57	30.89	30.98	35.20	20.68	20.25	44.52
Avast Software avast!	7.38	18.51	10.28	148.65	30.64	8.16	38.56	64.01	23.76	72.82	40.03	8.07	45.54
Avertive VirusTect	20.61	28.83	28.72	191.13	47.08	47.11	46.29	4.56	4.55	61.06	3.35	3.37	52.42
AVG Internet Security	10.39	0.66	0.01	3.66	32.99	5.60	5.20	63.56	18.79	23.11	91.50	14.96	27.49
Avira AntiVir Server	23.16	6.24	4.15	37.43	20.55	7.42	20.44	42.29	29.23	41.11	42.70	43.48	41.89
BitDefender Security	16.61	146.80	1.41	147.60	38.76	4.48	38.93	62.40	15.64	62.38	64.77	3.71	65.44
Bkis BKAV Professional	72.62	8.33	8.43	NA	66.38	66.24	66.38	129.71	127.54	129.71	175.27	175.70	175.27
Bullguard AntiVirus	26.69	94.67	1.46	NA	45.05	4.94	45.05	80.11	20.90	80.11	82.33	11.20	82.33
CA Total Defense	6.52	4.92	0.36	292.85	15.29	2.75	16.37	22.46	4.82	25.12	57.79	31.52	61.66
Central Command Vexira	19.98	4.36	2.60	5.82	46.96	23.15	22.66	55.99	39.26	51.86	113.72	44.45	56.14
Clearsight Antivirus	21.26	36.77	36.68	196.95	59.51	59.53	58.48	26.80	26.57	86.31	15.74	15.83	73.52
Commtouch Command	41.86	149.89	97.05	107.35	70.75	71.85	66.33	142.32	137.44	132.24	108.00	94.41	87.63
Coranti 2010	28.79	12.80	12.74	17.32	78.30	78.30	77.88	67.87	67.27	100.40	75.33	75.12	99.50
Defenx Security Suite	181.55	20.12	193.78	NA	77.11	806.57	77.11	1035.12	4712.22	1035.12	2302.01	7321.08	2302.01
Digital Defender	21.10	28.58	28.88	184.51	47.18	47.01	43.33	4.74	4.55	48.36	22.69	21.01	77.73
eEye Blink Server	60.78	4.92	5.27	603.16	90.46	91.76	88.80	180.39	178.73	178.47	265.84	264.91	266.12
Emsisoft Anti-Malware	4.44	0.01	0.01	NA	8.44	4.68	8.44	11.63	12.42	11.63	12.60	9.28	12.60
eScan ISS	21.74	6.79	2.18	NA	21.93	7.15	21.93	49.23	11.40	49.23	27.29	7.72	27.29
ESET NOD32	2.03	3.53	3.53	3.43	3.94	4.01	13.16	54.71	54.72	54.33	31.51	31.44	42.27
Fortinet FortiClient	54.43	103.54	3.17	103.54	90.66	7.88	90.66	48.85	11.51	48.85	72.49	7.87	72.49
Frisk F-PROT	35.60	6.94	14.79	NA	66.55	67.93	66.55	24.25	23.97	24.25	55.96	37.75	55.96
F-Secure PS	25.68	0.49	0.55	554.00	49.43	37.96	55.18	72.42	71.42	92.20	106.24	87.35	137.97
G Data AntiVirus Client	28.87	45.29	2.29	45.29	64.62	7.59	64.62	104.59	15.29	104.59	117.87	12.01	117.87
Ikarus virus.utilities	14.13	51.00	51.00	NA	45.27	44.94	45.27	42.95	43.02	42.95	40.67	39.71	40.67
Kaspersky Small Office	0.49	5.57	4.79	232.25	26.01	0.01	28.18	42.85	6.03	46.82	50.25	0.01	53.21
Keniu Antivirus	22.09	5.08	5.12	9.59	38.92	38.70	39.05	27.13	26.69	56.49	15.65	15.91	71.00
Kingsoft AntiVirus Adv. A	15.09	1.54	0.01	NA	33.74	6.52	33.74	110.07	14.80	110.07	45.27	10.07	45.27
Kingsoft AntiVirus Adv. B	2.83	0.56	0.01	NA	4.73	4.64	4.73	12.43	12.31	12.43	9.26	8.94	9.26
Kingsoft AntiVirus Std	15.74	3.55	1.47	NA	28.34	5.87	28.34	112.82	18.64	112.82	39.44	4.19	39.44
Lumension EMSS	120.01	7.72	7.55	NA	97.93	97.83	NA	217.15	216.89	NA	265.47	268.49	NA
Microsoft Forefront	16.74	5.68	2.20	NA	59.70	7.09	59.70	35.03	10.77	35.03	46.09	6.53	46.09
Mongoosa	19.27	6.96	2.21	NA	56.24	7.09	56.24	81.44	11.12	81.44	189.04	7.25	189.04
Norman Security Suite	98.17	6.51	6.47	NA	92.38	92.46	92.38	206.95	206.27	206.95	254.78	254.38	254.78
Preventon Antivirus	20.84	29.14	29.16	190.90	47.16	47.10	46.47	4.60	4.58	60.95	3.24	3.55	54.56
Quick Heal AntiVirus	7.23	33.80	7.62	NA	13.19	2.84	13.19	74.74	8.94	74.74	59.97	2.54	59.97
Returnil System Safe	43.19	21.84	21.78	NA	64.01	65.00	64.01	135.72	132.41	135.72	64.70	64.59	64.70
Sophos ESC	25.13	4.26	4.28	561.89	41.26	40.49	47.80	13.12	11.66	18.52	66.92	65.19	76.39
SPAMfighter VIRUSfighter	22.48	35.73	35.63	135.67	59.42	59.41	58.60	26.73	26.71	84.80	15.72	15.56	72.33
GFI/Sunbelt VIPRE	6.61	0.31	0.01	NA	32.28	0.90	32.28	543.38	0.01	543.38	656.84	27.04	656.84
TGSoft VirIT eXplorer	44.13	5.57	4.54	NA	32.80	29.92	32.80	17.69	17.30	17.69	16.44	16.53	16.44
Trustport Antivirus 2011	28.29	13.26	0.01	640.54	91.27	8.54	93.65	135.95	43.50	155.55	201.67	17.64	254.87
VirusBuster	37.85	4.28	2.77	5.59	54.95	35.03	34.36	48.27	48.79	61.03	116.07	61.97	74.35

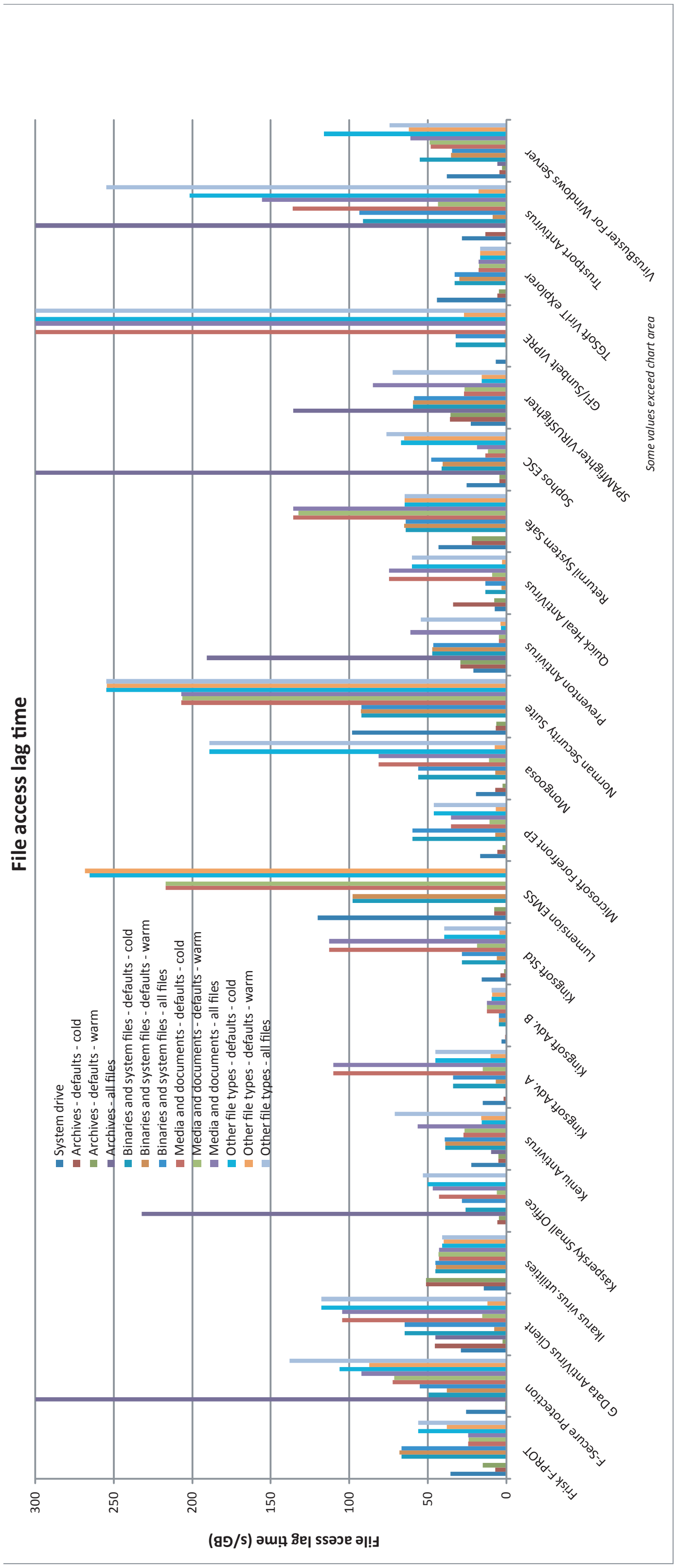
* System drive measure shows the average throughput of two runs over the system (C:) partition using default settings – one 'cold' and one 'warm' run.

(Please refer to text for full product names.)

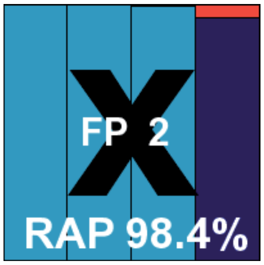


Some values exceed chart area

(Please refer to text for full product names.)



(Please refer to text for full product names.)



Still hanging onto the 2010 name, *Coranti*'s product includes a swathe of engines for extreme protection. *F-PROT*, *BitDefender* and *Lavasoft* are listed as the main providers, but the *GFI/Sunbelt* engine is also included via *Lavasoft*. The product itself is a fairly compact 47MB, and set itself up in good time, but online updates took rather a long time as usual.

The interface is text-heavy but logically laid out, with clearly marked controls, and provides an excellent degree of fine-tuning. Operation was steady and well-behaved, and testing completed well within the expected time frame.

Scanning speeds were a little on the slow side, and lag times a little heavier than most (unsurprisingly for a multi-engine product). While CPU use was a little high, RAM consumption was not unreasonable and impact on our set of tasks was not too heavy either.

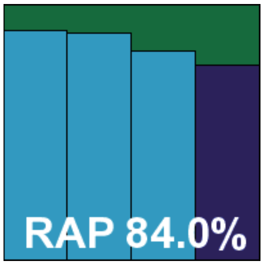
Detection rates were of course superb – close to perfect in most areas and with only the slightest drop in the proactive week of the RAP sets. The WildList set was brushed aside with ease, but in the clean sets the two expected false alarms appeared, as we could have predicted from previous products including the *F-PROT* engine, and *Coranti* is denied a VB100 award this month. Having entered six of our comparatives now, *Coranti* has two passes, both in the last year.

Defenx Security Suite 2011

Version 2011 (3390.519.1248)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	91.38%
Worms & bots	95.34%	**False positives**	0

vb
100
VIRUS
virusbtn.com
June 2011



Defenx is an adaptation of the *Agnitum* suite with some extras of its own, and has a similar set-up process. The 109MB installer runs through without complications and needs a reboot to complete. The interface is clear and lucid with good usability and a reasonable degree of controls for the anti-malware component, much of the GUI space being given over to firewall settings.

Once again things ran much more slowly than we are used to from *Defenx*, with some of the large scans taking several days to complete (a scan of our standard test sets, not including the RAP or clean sets, took a total of six days). Most of the on-demand speed measures were abandoned after the allotted two hours (many other products managed most of these jobs in less than ten minutes). Thinking perhaps there was something wrong with the install we retried on a different system but saw the same results. On-access lag times were also extremely heavy, and along with pretty high CPU consumption our set of activities was considerably slower to run than we would expect.

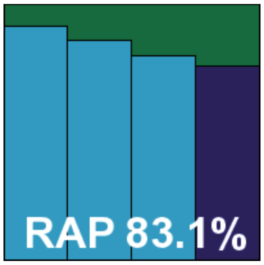
With the results finally in – after almost two full weeks of precious machine time – we saw some reasonable detection rates, with no problems in the clean sets and the WildList capably handled, earning *Defenx* a VB100 award. Although we saw no signs of instability or flakiness, the extreme slowdown is something of a concern, and hopefully the developers will diagnose the problem quickly. The company has a good record in our tests since joining just over a year ago, with seven passes and a single test not entered in the last eight comparatives.

Digital Defender

Version: 2.1.56, Definitions date: 18/04/2011, Definitions version: 13.6.311

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.53%
Worms & bots	94.24%	**False positives**	0

vb
100
VIRUS
virusbtn.com
June 2011



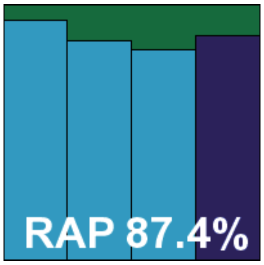
Another member of the *Preventon* club, with a longer history of participation than many, *Digital Defender* has a similar install process, with its 74MB executable running through in good time and not needing a reboot. Once again it was updated online with the date shown a couple of days before the update was actually run. The GUI is clear and usable, and in the past has shown admirable solidity and good behaviour. This time, however, we observed a number of issues handling our on-access tests, with the protection apparently shutting off silently part way through the runs. After several attempts we managed to get a complete set of results though.

Scanning speeds were reasonable, with light lag times, low use of RAM and low impact on our set of tasks; CPU use was a little higher but far from bad. Detection rates were reasonable, and the core certification requirements were met, earning *Digital Defender* another VB100 award. This seems to indicate the end of a run of bad luck for the company, which now has two passes from five entries in the last year, three from seven entries in the eight tests since its first appearance.

eEye Blink Server

Version 4.8.1, Rule version 1616, AntiVirus version 1.1.1492

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	95.99%
Worms & bots	96.32%	**False positives**	0



Another semi-regular entrant, *eEye*'s server edition came as a fairly large 192MB installer with an additional 107MB of updates. The set-up is fairly lengthy, with several long pauses while components are prepared and configured and a fair number of steps to click through. No reboot is needed at the end however, and the user is led straight into a configuration wizard.

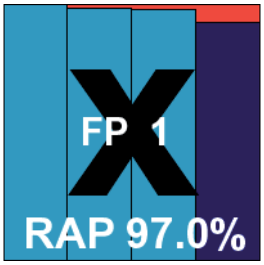
The interface differs from the standard desktop product in having a sober grey background, although the install system is daubed in a rather fruity salmon pink. The layout is fairly pleasant and in general straightforward to operate, with a reasonable level of configuration available. The product ran fairly smoothly in general, although one scan did seem to give up after a couple of days' hard work. Scanning speeds were on the slow side, although they never threatened to over-run our time limits, and on-access lag times were quite high too, but our set of tasks ran through in good order and RAM consumption was low, if processor drain was a little high.

Detection rates were pretty solid, with decent levels in all sets, and the WildList and clean sets were managed ably, earning *eEye* a VB100 award. This is the vendor's third pass from four entries in the last year – another product showing signs of recovery after a rough patch; its two-year history shows four passes from eight entries.

Emsisoft Anti-Malware for Server

Version 5.1.0.10

ItW	100.00%	**Polymorphic**	95.61%
ItW (o/a)	100.00%	**Trojans**	99.17%
Worms & bots	99.64%	**False positives**	1



Emsisoft's 99MB install package – containing all required updates – ran through with a very slick and professional feel, completing in good time with no need to reboot. The interface is a little more quirky, with some rather disconcerting menus which do not go away when you might expect them to, but is generally fairly clear and usable. Testing proved generally fairly straightforward, but we did encounter a few issues in the on-access tests, with the protection apparently shutting down from time to time when under heavy load.

After a few repeat runs we managed to get a full set of results though, showing some rather sluggish scanning times but very low overheads in the on-access runs. RAM use was very low and CPU consumption well below average too, but impact on our activities set was a little higher than most.

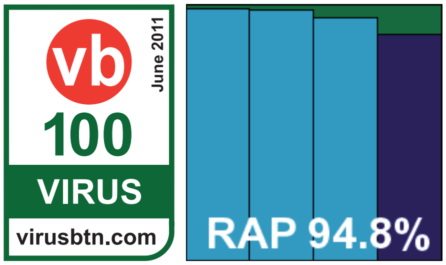
Detection rates were excellent though, with well over 90% in all areas, even the proactive week of the RAP sets. The WildList was handled well, but in the clean sets a single item – oddly an index web page from one of the magazine cover CDs added this month – was alerted on as malicious, and *Emsisoft* just misses out on VB100 certification. The vendor has had something of a tough time in our comparatives, with two passes from five entries in the last year; four fails and two tests skipped since its first entry eight tests ago.

eScan Internet Security Suite

Version 11.0.139.964

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	98.97%
Worms & bots	99.76%	**False positives**	0

One of our most consistent participants, *eScan*'s desktop product is very familiar to the lab team, and running the 164MB installer presented no difficulties (although it did take some time setting up the wide range of components included in the suite). The interface seems a little curvy and glitzy for a business environment, but is pleasant to use with plenty of controls under the glossy surface.



Initial tests ran well, with no signs of instability in on-access measures, but on-demand scans were considerably more problematic. Speed tests showed no sign of ever finishing, and all were abandoned after over-running the two-hour time limit.

Scanning of our infected sets was similarly snail-like, with the standard sets (which account for about a quarter of the total data needing to be scanned) taking 279 hours to get through. Fortunately much of this was while the team were absent from the lab, but still with other tests to run the product took up close to 30 full days of testing time – basically hogging one of our seven test systems for the entire month.

Clean set scans were abandoned after running overnight and only covering a few thousand files. Logs kindly reported how long each file had taken to deal with, in some cases reporting several minutes for a single small file – but at this rate we would never have got through the full 450,000 or so samples in the set, so the test was run using the on-access component, which seemed to run perfectly happily. The main sets, having taken 12 days on demand, were processed in under two hours on access.

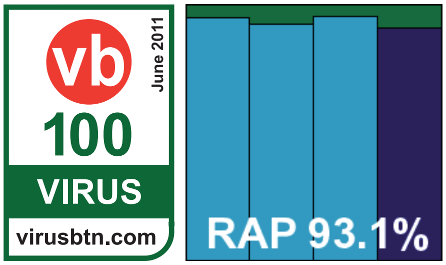
This odd dichotomy is demonstrated in our speed charts, which show barely visible on-demand speeds but quite acceptable, even fairly low overheads on access. RAM use may be slightly higher than average, but our set of activities ran through in short order.

After all this, detection rates proved as solid as ever, with good scores across the board. The core certification sets were handled cleanly, albeit extremely slowly in some cases, and a VB100 award is just about earned. Hopefully the developers will sort out this issue rapidly though, as few users would be happy to leave scans running for weeks at a time. The historical view shows four passes and two fails in the last year, nine of the last dozen tests passed with no tests skipped.

ESET NOD32 Antivirus 4

Version 4.2.72.0, Virus signature database 6058 (20110420)

ItW	100.00%	**Polymorphic**	99.99%
ItW (o/a)	100.00%	**Trojans**	94.38%
Worms & bots	96.35%	**False positives**	0



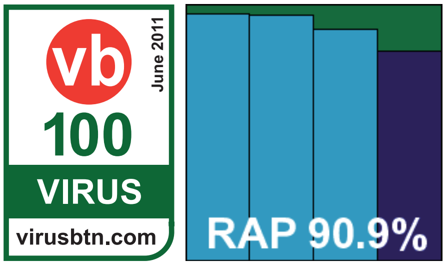
Another of our most regular participants, *NOD32* is a fixture on our product lists, and the current version has become a familiar and popular sight on the test bench. The install process for the compact 49MB product is fast and simple, enlivened by the unusual approach of forcing a decision on whether or not to detect grey items, and needs no reboot to complete. The GUI is sharp and funky without losing touch with good design or ease of use, and provides enormous levels of fine-tuning without becoming cluttered or confusing.

The tests ran through with dependable solidity, with fast scanning speeds and low lag times on access. RAM use was low and our set of tasks ran through rapidly, although processor use was higher than some. Detection tests showed some solid coverage of the sets, no problems in the core certification sets, and *ESET* once again earns a VB100 award. The vendor's record is exemplary, with all of the last 12 tests (indeed, all of the last 47 tests) entered and passed.

Fortinet FortiClient

Version 4.1.3.143, Virus signatures version 10.134, Anti-virus engine 4.2.257

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	93.76%
Worms & bots	97.09%	**False positives**	0

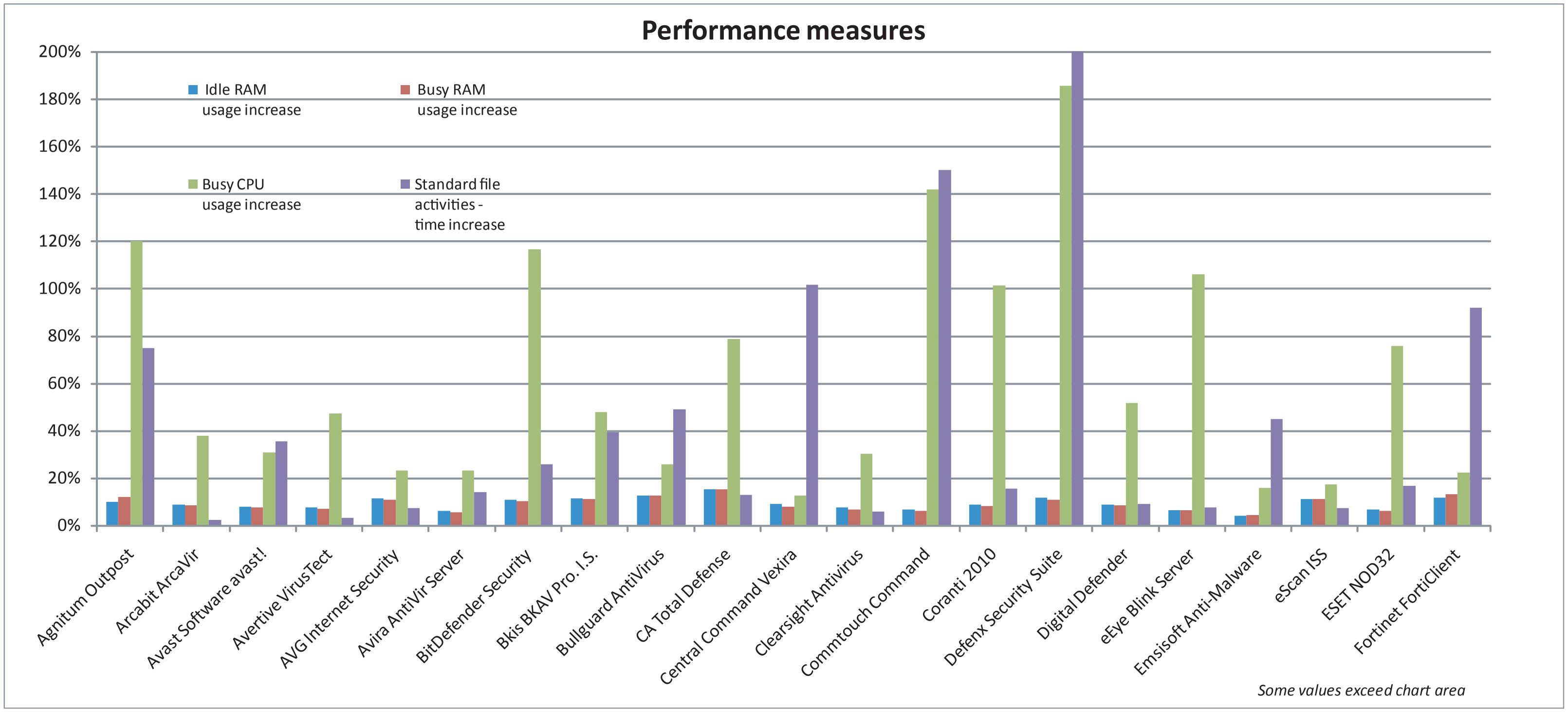


FortiClient is another very compact product, with the main installer measuring just 10MB, although updates were large at 133MB. The set-up process is simple and rapid, offering a choice of free or premium versions and completing in under half a minute.

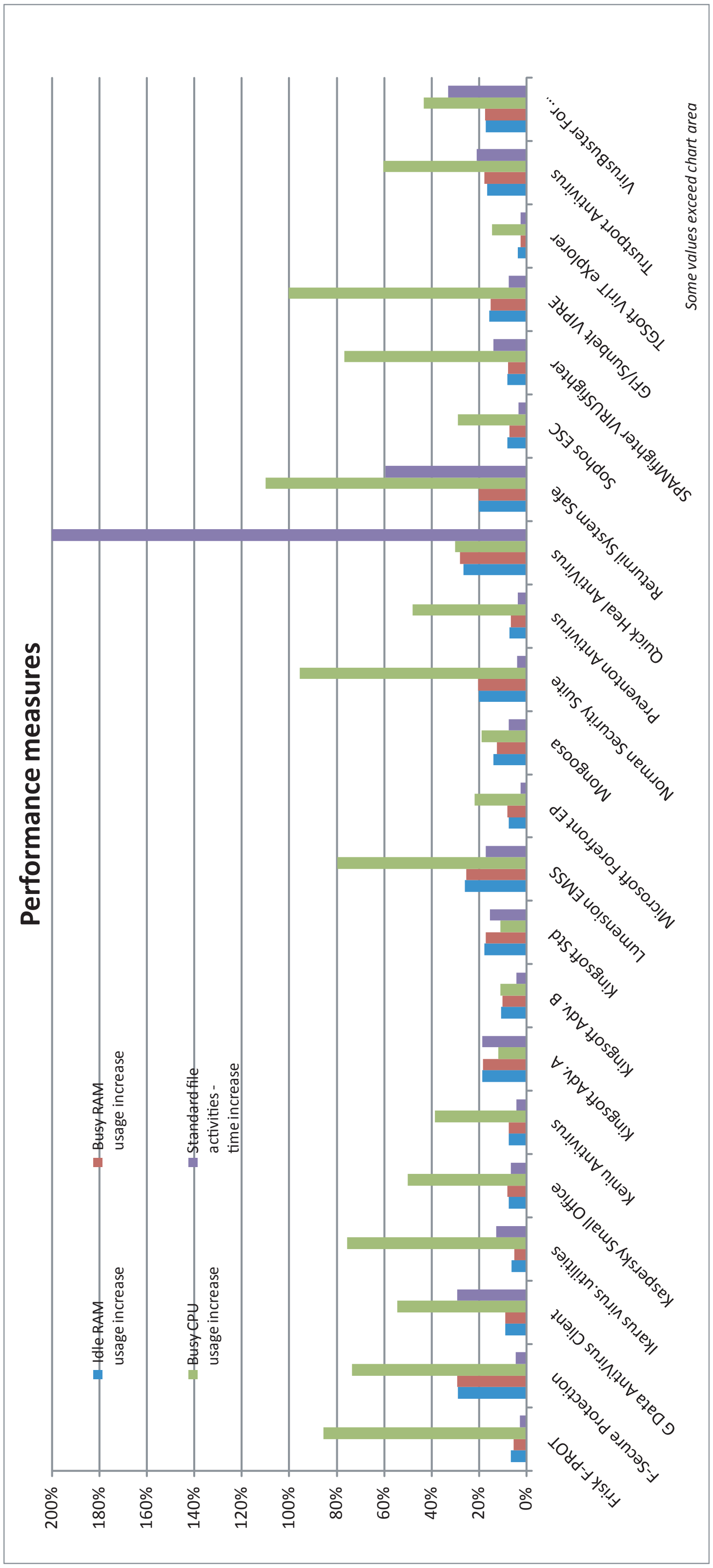
The interface is serious and businesslike, with none of the cutesy icons and cuddly cartoon logos favoured by more consumer-focused solutions. The layout is clear and lucid,

Performance measures	Idle RAM usage increase	Busy RAM usage increase	Busy CPU usage increase	Standard file activities – time increase
Agnitum Outpost Security Suite Pro	9.89%	11.99%	120.15%	74.73%
Arcabit ArcaVir 2011	8.89%	8.40%	37.78%	2.24%
Avast Software avast! 4.8	7.91%	7.75%	30.89%	35.57%
Avertive VirusTect	7.67%	6.96%	47.37%	3.18%
AVG Internet Security 2011	11.42%	10.77%	23.20%	7.40%
Avira AntiVir Server	6.27%	5.63%	23.22%	14.18%
BitDefender Security for File Servers	10.84%	10.26%	116.51%	25.74%
Bkis BKAV Professional I.S.	11.49%	11.25%	47.99%	39.32%
Bullguard AntiVirus	12.51%	12.77%	25.90%	49.15%
CA Total Defense r12 I.S.	15.23%	15.15%	78.70%	13.00%
Central Command Vexira	9.20%	8.01%	12.69%	101.65%
Clearsight Antivirus	7.54%	6.63%	30.34%	5.98%
Commtouch Command Anti-Malware	6.88%	6.10%	141.77%	150.05%
Coranti 2010	8.96%	8.34%	101.29%	15.67%
Defenx Security Suite 2011	11.81%	10.77%	185.52%	208.98%
Digital Defender	8.86%	8.55%	51.59%	9.20%
eEye Blink Server	6.39%	6.39%	106.10%	7.63%
Emsisoft Anti-Malware for Server	4.13%	4.53%	15.94%	44.86%
eScan Internet Security Suite	11.11%	11.10%	17.44%	7.31%
ESET NOD32 Antivirus	6.67%	6.25%	75.63%	16.73%
Fortinet FortiClient	11.80%	13.13%	22.25%	91.87%
Frisk F-PROT Antivirus	6.51%	5.38%	85.51%	2.53%
F-Secure Protection Service	28.83%	29.01%	73.33%	4.30%
G Data AntiVirus Client	8.73%	8.81%	54.39%	29.19%
Ikarus virus.utilities	6.03%	5.07%	75.55%	12.68%
Kaspersky Small Office Security	7.30%	7.80%	49.88%	6.52%
Keniu Antivirus	7.38%	7.34%	38.58%	4.10%
Kingsoft AntiVirus 2011 Advanced A	18.42%	18.07%	11.89%	18.49%
Kingsoft AntiVirus 2011 Advanced B	10.62%	9.95%	10.83%	4.07%
Kingsoft AntiVirus 2011 Standard	17.57%	17.10%	10.74%	15.40%
Lumension EMSS	25.96%	25.22%	79.54%	16.97%
Microsoft Forefront Endpoint Protection 2010	7.46%	7.91%	21.82%	2.27%
Mongoosa	13.68%	12.35%	18.81%	7.21%
Norman Security Suite	20.08%	20.27%	95.38%	3.95%
Preventon Antivirus for Server	7.00%	6.32%	48.01%	3.57%
Quick Heal AntiVirus 2011 Server Ed.	26.33%	27.76%	30.10%	2117.03%
Returnil System Safe 2011	20.05%	20.00%	109.95%	59.30%
Sophos Endpoint Security and Control	7.84%	6.99%	28.87%	3.28%
SPAMfighter VIRUSfighter	7.92%	7.60%	76.54%	13.83%
GFI/Sunbelt VIPRE Antivirus	15.47%	14.94%	100.27%	7.33%
TGSoft VirIT eXplorer PRO	3.43%	2.48%	14.49%	2.24%
Trustport Antivirus 2011	16.51%	17.65%	60.21%	20.73%
VirusBuster For Windows Server	16.99%	17.39%	43.03%	32.85%

(Please refer to text for full product names.)



(Please refer to text for full product names.)



(Please refer to text for full product names.)

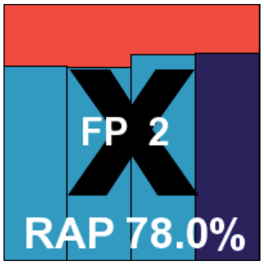
with no room for confusion and all required controls are placed within easy reach. Operation proved solid and stable, powering through our tests without a snag or hiccup. Scanning speeds were decent and lag times not too bad either, but our set of tasks took a little longer than usual to run through.

Detection rates were good, showing continued improvement, and the core requirements were met with ease, earning *Fortinet* a VB100 award. *Fortinet*'s history is something of a roller coaster, but shows the fruits of its recent improvements, with four passes from five entries in the last year; the two-year view shows seven passes from 10 entries.

Frisk F-PROT Antivirus for Windows

Version 6.0.9.5, Scanning engine 4.6.2

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	77.19%
Worms & bots	82.37%	**False positives**	2



Frisk's products are rarely absent from our list of participants, and the vendor's engine continues to be popular with OEM developers. From a couple of results already discussed, things looked decidedly gloomy for *Frisk* this month.

The installer is a small 31MB MSI file, accompanied by a 60MB update package. The set-up process is short and simple, with only a few clicks and a few seconds' wait before a reboot is requested to complete the job. The interface is similarly uncomplicated, with minimal fine-tuning but admirable usability. Stability seemed fine throughout the test, all jobs completing well within the expected time.

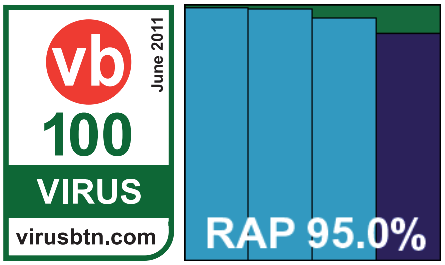
Scanning speeds were not bad, and overheads fairly light, with very low use of system memory and barely any effect on our set of tasks (although CPU use was quite high at busy times).

Detection rates were reasonable, oddly increasing slightly in the later parts of the RAP sets, and the WildList was covered flawlessly. As expected though, a couple of items in the clean set were labelled malicious, including that *iTunes* installer, and *Frisk* doesn't quite make the grade for VB100 certification this month. In the last six tests, *Frisk* now has four passes and two fails, with seven passes in the last two years, during which time no tests have been missed.

F-Secure Protection Service

Version 9.00 build 198, Anti-virus version 9.20 build 16050

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.13%
Worms & bots	99.77%	**False positives**	0



F-Secure's server protection suite came as a fairly compact 75MB main installer, accompanied by 132MB of updates. The install process is speedy and simple, all completed in under a minute with no need to reboot. Being web-based, the interface is a little different from the norm and is quite fiddly on this platform as the default browser controls block access to the locally hosted page to start with. Once this is sorted out the GUI is fairly usable, but can be rather slow to respond at times, causing the occasional moment of confusion when a message insisting changes need to be applied is shown right after the 'apply' button has been clicked. We also saw the machine become very slow to respond for quite long periods after changes to the settings were made, and at one point saw a recurrence of previous issues with logs failing to generate properly.

Scanning speeds were not bad, but on-access lag times were a little on the high side. A lot of RAM was taken up by the product, and CPU use was a little high too, but our set of activities got through in good time. Detection rates were splendid though, with excellent scores everywhere, only the latest week of the RAP sets showing any decline in coverage. The WildList and clean sets were handled fine, and a VB100 award is duly earned by *F-Secure*. The company's long-term view shows a fairly regular pattern of entries, with four passes from four entries in the last six comparatives; eight from eight in the last two years.

G Data AntiVirus Client

Client 10.5.132.28, AVA 22.284, AVB 22.47

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.77%
Worms & bots	99.97%	**False positives**	1

G Data's business product is a complete package, with a sophisticated management system controlling clients. The

Archive scanning		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Agnitum Outpost Security Suite Pro	OD	2	√	√	X	√	X	√	X	√	X	√
	OA	X	√	√	√	√	X	√	X	√	X	√
Arcabit ArcaVir 2011	OD	2	√	√	√	√	√	√	√	√	1	√
	OA	X/2	X/√	√	√	X/√	X/√	X/√	X/√	X/√	X/1	√
Avast Software avast! 4.8	OD	X/√	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 Internet Security 2011	OD	√	√	√	√	√	√	√	√	√	√	X/√
	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 for File Servers	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	8/√	8/√	4/√	4/√	8/√	8/√	8/√	4/8	8/√	8/√	√
Bkis BKAV Professional I.S.	OD	X	X	X	X	X	X	X	X	X	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Bullguard AntiVirus	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	2	2	1	1	2	2	2	1	2	2	√
CA Total Defense r12 I.S.	OD	X	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	X/√	√
	OA	X	X/√	X/√	X/√	1/√	X/√	X/√	X/√	1/√	X/√	√
Central Command Vexira	OD	X	√	√	√	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		1	X/1	X/√
Commtouch Command Anti-Malware	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	√
Coranti 2010	OD	√	√	8	8	√	√	√	8	√	√	√
	OA	X/1	X	X	X	X/√	X	X	X	1	X/1	X/√
Defenx Security Suite 2011	OD	2	√	√	√	√	X	√	√	√	X	√
	OA	X	X	X	X	X	X	X	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	X	1	1	1	1	1	1	2/√	2	X	√
	OA	X	X/√	X/√	X	X/√	X/√	X/√	X/√	X/√	X	√
Emsisoft Anti-Malware for Server	OD	2	2	2	2	2	2	2	3	2	2	√
	OA	2	2	2	2	2	2	2	X	2	2	√
eScan Internet Security Suite	OD	√	7	6	4	7	7	7	7	8	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
ESET NOD32 Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Fortinet FortiClient	OD	X	√	√	√	√	√	√	√	√	1	√
	OA	X	√	√	√	√	√	√	√	√	1	√

Key:

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

X - No detection of EICAR test file

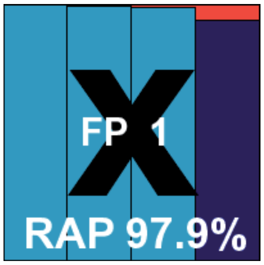
X/√ - defaults settings/all files

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

* - Detection of EICAR test file with randomly chosen (non-executable) file extension

OD/OA - On Demand/On Access

(Please refer to text for full product names.)



installation process is thus a little more complex than most, with the client system needing to be installed first, with associated database tools etc., and then protection deployed to the local system. This proved a reasonably straightforward process though, with the interface laid out in a clear and perfectly usable manner, allowing us to perform all the required jobs without recourse to manuals or needing to rummage around in control systems. The only confusion came when the product tried to install the .NET framework and was blocked from doing so by the platform, which insisted such things be installed via the built-in role management system. This was soon dealt with though, and having set up the required policies in the MMC console tool, we were able to run most tasks from the client side, despite the relatively basic nature of the tools provided at this level.

The speeds sets were scanned in reasonable time at first sight, and ripped through at lightning pace on repeat runs. Similarly splendid optimization took place on access too, making for some very light overheads. Resource use remained very reasonable, and our suite of tasks took a little longer than usual but not excessively so.

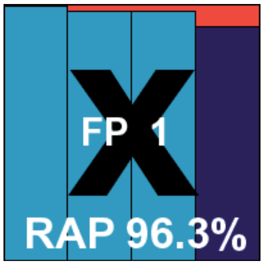
Detection rates were as magnificent as ever, with almost impeccable scores in most sets. The WildList was easily covered, but in the clean sets a single item was mislabelled as malware – a little oddly given that neither of the main engines powering the product detected the item in their standalone incarnations. Nevertheless, it was enough to deny *G Data* a VB100 award despite an otherwise excellent performance. The vendor's history shows some bad luck in the last year, with two fails and three passes, the *Linux* test being a non-entry; the longer view is a little better, with eight passes from ten entries in the last dozen tests.

Ikarus virus.utilities

Product version 2.0.15, Scan engine version 1.1.103, Virus database 78206

ItW	100.00%	**Polymorphic**	95.61%
ItW (o/a)	100.00%	**Trojans**	99.07%
Worms & bots	99.44%	**False positives**	1

As usual, *Ikarus* provided its product as an iso image of a complete install CD, making it rather large at 200MB. The actual installation process is fast and simple though, and was all completed in under a minute with no need to restart the system.



The interface is fairly rudimentary – a rather rough-and-ready .NET affair – but offers a fair amount of controls and is reasonably easy to navigate and operate. The speed tests progressed well, with good scanning times and reasonable lag times, low use of RAM and low impact on our set of tasks but fairly high CPU use. However, attempting to run the simple archive detection test brought up a serious problem. The scan – covering a selection of simple archives containing the EICAR test file – completed without a problem, but on clicking the button to display the results, the interface froze up completely and refused to respond to any stimulus. On rebooting the machine, after the initial *Windows* splash screen the screen remained blank, with just a stationary cursor pointer, failing to progress to full operation. We found that not even safe mode could get the machine to boot up, and the system had to be scrapped and re-imaged. However, after re-running several variants on the same set of actions, we failed to reproduce the problem.

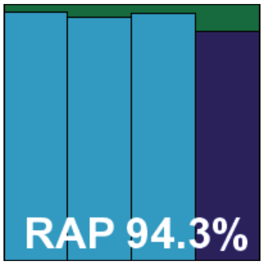
The second install got through the rest of the tests without any more nasty surprises, and in the end the usual excellent detection rates were produced, including perfect coverage of the WildList set. The clean sets yielded the same false alarm seen with a partner product though, and *Ikarus* doesn't quite make the grade for VB100 certification this month. Things are still looking up for *Ikarus* though, with two passes from four entries in the last year; two from six tries in the last 12 tests.

Kaspersky Small Office Security

Version: 9.1.0.59

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	95.27%
Worms & bots	98.89%	**False positives**	0

vb 100 VIRUS virusbtn.com June 2011



This month's submission from *Kaspersky* was a new one to us, apparently a small business equivalent of the company's *PURE* product line. The installer is a largish 214MB and the updates provided weighed in at a hefty 173MB, although this

Archive scanning contd.		ACE	CAB	EXE-RAR	EXE-ZIP	JAR	LZH	RAR	TGZ	ZIP	ZIPX	EXT*
Frisk F-PROT Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X	2	2	X	X	X	2	2	√
F-Secure Protection Service	OD	X/√	√	√	√	√	√	√	8	√	X/√	X/√
	OA	X/√	X/√	X	X	X/√	X/√	X/√	X/8	X/√	X/√	X/√
G Data AntiVirus Client	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	√	√	3/9	4/√	√	√	√	8/√	8/√	√	√
Ikarus virus.utilities	OD	2	2	2	2	2	2	2	X	2	2	√
	OA	2	2	2	2	2	2	2	3	2	2	√
Kaspersky Small Office Security	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	1/√	1/√	X/√	X/√	X/√	X/√	X/√	X/√	√
Keniu Antivirus	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X	X	X/1	X/1	X	X	X	X	X	X	X/√
Kingsoft AntiVirus 2011 Advanced A	OD	X	√	√	X	√	√	√	√	√	1	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kingsoft AntiVirus 2011 Advanced B	OD	X	√	√	√	√	X	√	X	√	√	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Kingsoft AntiVirus 2011 Standard	OD	X	√	√	X	√	√	√	√	√	1	√
	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	X
Microsoft Forefront Endpoint Protection	OD	√	√	√	√	2	2	2	√	√	√	√
	OA	X	X	X	1	X	X	X	X	1	X	√
Mongoosa	OD	1	1	1	1	1	X	1	X	1	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Norman Security Suite	OD	X	√	√	1	√	√	√	√	√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Preventon Antivirus for 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 AntiVirus 2011 Server Ed.	OD	X	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 2011	OD	5	5	5	5	5	√	5	2	5	5	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Sophos Endpoint Security and Control	OD	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/√
	OA	X	X/5	X/5	X/5	X/5	X/5	X/5	X/5	X/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/√
GFI/Sunbelt VIPRE Antivirus	OD	X	X	√	√	√	X	√	X	√	1	√
	OA	X	X	√	√	X	X	X	X	X	X	√
TGSoft VirIT eXplorer PRO	OD	X	X	X	X	X	X	X	X	X/√	X	√
	OA	X	X	X	X	X	X	X	X	X	X	√
Trustport Antivirus 2011	OD	√	√	√	√	√	√	√	√	√	√	√
	OA	X/√	X/√	X/√	X/√	√	X/√	X/√	X/√	1/√	1/√	√
VirusBuster For Windows Server	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/√ - defaults settings/all files

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

* - Detection of EICAR test file with randomly chosen (non-executable) file extension

OD/OA - On Demand/On Access

(Please refer to text for full product names.)

included data for the whole product range. The install process is smooth and attractive, running through the usual steps including the option to participate in a feedback scheme, and completing in under a minute with no need to restart.

The interface closely resembles the company's consumer lines, but in a sensible grey colour scheme for business use. The design has a few quirks, but is generally very clear and simple to use, with a complete range of fine-tuning controls at the user's fingertips. Running through the tests proved painless, with the product showing its usual solid stability throughout.

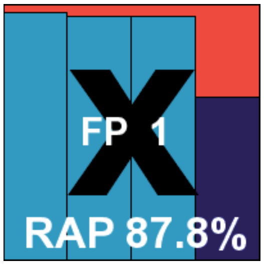
Scanning speeds were impressive from the off, and sped up to extreme pace on repeat runs, with similar optimization on access making for minimal lag times. Memory consumption was low, and our tasks zipped through very rapidly. While CPU use was a little higher than some products, it was far from excessive.

Detection rates were extremely good across the board, just dipping a little in the proactive week of the RAP sets, and the core certification requirements were met without difficulty, earning *Kaspersky* another VB100 award. The company's test history shows five passes and a single fail in the last six tests; nine passes, two fails and a single non-entry (the only VB100 comparative ever not to feature a product from *Kaspersky*) in the last two years.

Keniu Antivirus

Program version 1.0.5.1142

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	76.50%
Worms & bots	98.95%	**False positives**	1



Keniu has always been something of a conundrum: the product is ostensibly based on the *Kaspersky* engine but often shows lower than expected detection levels. The installer is a fairly sizeable 106MB (which includes all required updates) and sets up in super-quick time, with just a couple of clicks and a quick check of the system. No reboot is needed to finish off.

The interface is simple and minimalist, with little text and just a few large buttons covering the basic functions, although a few extra controls are provided under the covers. Initial tests progressed well, showing some slightly sluggish scanning times, fairly light on-access lag times, low impact on system memory and our set of activities and unexceptional use of processor cycles. Running through the infected sets proved a little more tricky though, with initial runs through the main sets showing large numbers of items not blocked. On demand, things proved even more difficult, with no sign of any logging whatsoever. A fresh install on a different test machine proved more successful though, with the logging all present and correct, and detection improved to cover the items that had initially been missed.

On the second attempt, scores still seemed a little odd, with lower rates than expected in our set of trojans, and excellent showings in the first parts of the RAP sets but a very steep drop into the proactive week. Re-runs showed the same results however. The WildList was handled properly after the initial problems had been resolved, but in the clean sets a single item – a system analysis tool provided by *Microsoft* – was labelled rather vaguely as malware, and *Keniu* is denied a VB100 award this month. Having now entered five tests in the last year, *Keniu* remains on three passes.

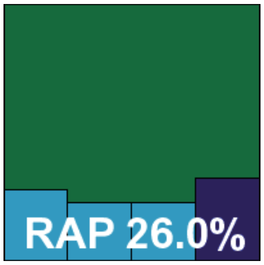
Kingsoft AntiVirus 2011 Advanced A

Program version: 2008.11.6.63, Engine version 2009.02.05.15, Data stream 2007.03.29.18, Virus definitions 2011.04.21.16

ItW	100.00%	**Polymorphic**	96.04%
ItW (o/a)	100.00%	**Trojans**	33.70%
Worms & bots	45.27%	**False positives**	0

The first in the usual triple bill from *Kingsoft*, the 'Advanced-A' edition is much as we have come to expect from the company – identical to previous entries whether labelled 'advanced' or 'standard'. The installer goes through the standard stages and runs through fairly quickly, ending with no need to reboot and leading into a basic set-up wizard.

vb 100 VIRUS virusbtn.com June 2011



The GUI is simple but nice and clear, using the most standard layout for such products and is thus easy to use from the off. Buttons are responsive and well marked, and there is a reasonable degree of configuration available.

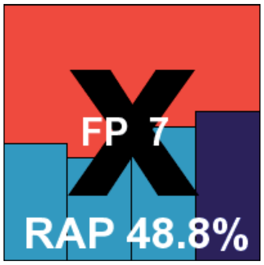
Running through the speed tests, scanning times were not too bad and overheads not too heavy, and although RAM use was fairly high, CPU drain was minimal and our set of activities completed very rapidly.

Detection rates, on the other hand, were pretty poor, with fairly low scores in most of our standard sets and woeful figures in the RAP sets. The WildList was handled better however, and with no false positives *Kingsoft* just about makes the grade for VB100 certification with the 'advanced' solution. In the last year, five entries have yielded only two passes, although the product has managed six passes from 10 entries in the last 12 tests.

Kingsoft AntiVirus 2011 Advanced B

2011.SP7.042017, 2011.04.21.16

ItW	100.00%	**Polymorphic**	95.89%
ItW (o/a)	100.00%	**Trojans**	61.07%
Worms & bots	59.50%	**False positives**	7



Having learned to expect a clutch of matching products from *Kingsoft*, this one threw a sizeable spanner in the works, being not only a completely redesigned product but also provided as a Chinese-language version. This made a lot of our work rather like groping around in the dark, but we managed to get it installed and running without excessive difficulties, even running through the bulk of the tests without needing to request help from the developers.

Gathering the scanning speed measures was the easiest task, and here we saw considerable improvement over the previous offering. On access was a little more tricky however, as there seemed to be no on-read protection, only on-write. This accounts for the low lag times in our standard measures, and also in part for the rapid processing of our set of standard jobs. Memory and CPU use were also lower than for the usual *Kingsoft* products.

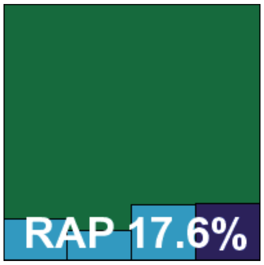
Detection tests were a little more tricky, but we eventually found the logging system. This proved misleading at times however, as the length of logs appeared to be capped at an arbitrary level, with data recorded longer than a certain amount of time ago thrown out. This caused considerable confusion, as the interface would show the results of a running scan not in complete terms, but only in reference to what was recorded in the logs – meaning that the number of items spotted in a scan could actually decrease as older detections were forgotten about.

Breaking the tests up into smaller jobs solved the issue though, and showed considerably better levels of detection than the product's stable mates, approaching respectable levels in the main sets but still a little disappointing in the RAP sets. With the WildList covered cleanly, the dangers associated with an increase in heuristic sensitivity reared their head in the clean sets, with a handful of false positives denying this product a VB100 award. According to the developers, this is a bleeding-edge trial though, and it certainly shows promise for the future.

Kingsoft AntiVirus 2011 Standard

Program version: 2008.11.6.63, Engine version 2009.02.05.15, Data stream 2007.03.29.18, Virus definitions 2011.04.21.16

ItW	100.00%	**Polymorphic**	96.03%
ItW (o/a)	100.00%	**Trojans**	19.34%
Worms & bots	36.70%	**False positives**	0



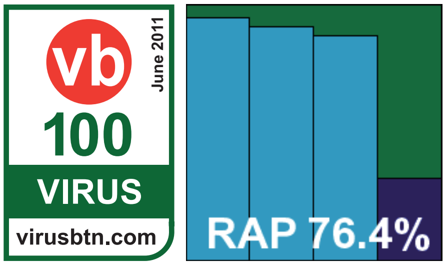
Somewhat confusingly, the 'Standard' edition of *Kingsoft*'s product line is identical to the 'Advanced-A' version in every respect (even down to the version information displayed). The set-up process and interface usage is identical, with similarly reasonable speed measures and low resource consumption, notably processor use. The only noticeable difference between the product versions was in their detection rates. Here, detection rates were even worse – missing huge swathes of our standard sets and barely registering in the RAP sets at all. Having met the core certification requirements, a VB100 award must be granted, but the product is clearly lagging well behind the rest of the field in terms of quality. Its history shows two passes from four entries in the last six tests; five from nine in the last two years.

Lumension Endpoint Management and Security Suite

Agent version 7.1.0.15, Scan engine version 6.7.7, AntiVirus definition files 6.7

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	96.41%
Worms & bots	96.69%	**False positives**	0

The first of a trio of new faces this month, *Lumension* is an Arizona-based firm specializing in vulnerability management



and whitelisting technologies. The product was provided as a 198MB installer, and set-up took quite some time, with a number of initial dependencies to resolve include *Microsoft*'s *Silverlight*. Despite the lab team's experience with security products, frequent reference to the installation guides was not enough and some support calls were required to get the full system up and running (help being needed mainly in navigating the management console, achieving online updates and deploying a protection agent to the local system). The product is a pretty thorough enterprise suite, including vulnerability management and compliance tools alongside anti-malware provided by the *Norman* engine.

The management system is operated from a web-based console, which suffers somewhat from the sluggish response that is common to such approaches. The complexity of the suite made it rather hard going to use at first, but with a little practice we figured out most of its quirks. A client-level agent tool seems mainly to provide information, with no local controls, so all jobs were run from the central management system. This provides a massive wealth of configuration but appears to be lacking some rather obvious standard items – such as the simple option to scan a given area. Scans can either encompass the entire local system or the whole system minus some exclusions, which must be defined using very specific syntax. An option is provided to import settings from a file, but with no information on how to create such a file we ended up going through the arduous process of setting up complex scan policies over and over again for our speed tests.

With a long list of exclusions in place to allow us to cover only the required areas we noted that, if left at its default setting of verbose logging of 'all scanned items', the scanner appears to go through the entire local system anyway, logging each file found and marking it as not scanned due to the exclusion policy. This obviously generated some rather large logs, and doubtless contributed to the less than stellar on-demand speed measures. On-access overheads were fairly high too, while use of memory and CPU were above average but not outrageous. Our suite of standard tasks completed in reasonable time, although the slowdown was clearly noticeable.

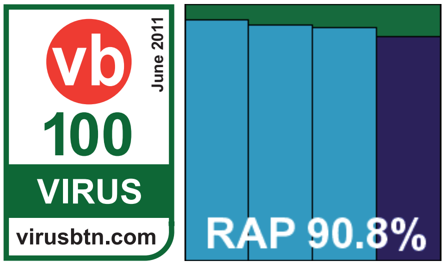
Getting through the infected sets took some time: almost a week all told. The log format is rather unusual but seemed a fairly efficient approach, although it proved tricky for our standard parsing tools to handle. Eventually we managed to harvest results which looked pretty decent in most areas – much as expected from the underlying engine – but the proactive week of the RAP sets looked completely out of balance. Re-running the job and analysing the logs more closely, we noticed that the scan seemed to be aborting only a short way through the set. Several repeat runs produced similar results. Even excluding the folder in which the scan was stopping failed to produce a full set of results, and having taken far more than its fair share of lab time we finally had to give up. Presumably, if spotted on their own, a far larger proportion of the samples in this set would have been detected, but something in there was clearly upsetting the scanning system and preventing it from showing its full capabilities.

Despite this, the WildList set was covered in its entirety and there were no problems in the clean sets – although in the speed sets (which are by design made up of only the most unthreatening files), a single suspicious item was alerted on. This does not prevent *Lumension* earning its first VB100 certification on its first attempt; it will be interesting to see if feedback from the developers renders future tests less hard work for us.

Microsoft Forefront Endpoint Protection 2010

Version: 2.0.0657.0, Antimalware client version: 3.0.8107.0, Engine version: 1.1.6702.0

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	90.87%
Worms & bots	97.86%	**False positives**	0



A much more familiar name, *Microsoft*'s *Forefront* is the second product this month to hang onto a 2010 label well in to 2011. While standard practice seems to dictate that 2012 versions will start to emerge pretty soon, *Microsoft*'s approach seems much more honest. The product is pretty compact with a 19MB installer and 64MB of updates, and the set-up process is fairly simple and speedy, with no need for a reboot.

The interface is pleasant and reasonably usable, providing a basic degree of configuration which in places is rendered a little fiddly thanks to some rather wordy labels on options.

Reactive And Proactive (RAP) scores		Reactive			Reactive	Proactive	Overall
		Week -3	Week -2	Week -1	average	Week +1	average
Agnitum Outpost Security Suite Pro	VIRUS 100	93.15%	88.70%	87.35%	89.73%	83.39%	88.15%
Arcabit ArcaVir 2011		67.00%	51.27%	58.16%	58.81%	59.29%	58.93%
Avast Software avast! 4.8	VIRUS 100	96.89%	92.88%	89.71%	93.16%	85.36%	91.21%
Avertive VirusTect	VIRUS 100	91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
AVG Internet Security 2011	VIRUS 100	97.50%	96.65%	95.20%	96.45%	88.41%	94.44%
Avira AntiVir Server	VIRUS 100	99.13%	87.60%	95.65%	94.12%	92.52%	93.72%
BitDefender Security for File Servers	VIRUS 100	99.37%	99.04%	98.91%	99.11%	93.32%	97.66%
Bkis BKAV Professional I.S.	VIRUS 100	99.46%	98.78%	99.03%	99.09%	95.13%	98.10%
Bullguard AntiVirus	VIRUS 100	99.37%	99.04%	98.97%	99.13%	93.39%	97.69%
CA Total Defense r12 I.S.	VIRUS 100	85.59%	76.81%	72.88%	78.42%	68.55%	75.96%
Central Command Vexira	VIRUS 100	90.97%	86.46%	85.13%	87.52%	80.84%	85.85%
Clearsight Antivirus	VIRUS 100	91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
Commtouch Command Anti-Malware		78.21%	78.33%	83.00%	79.85%	82.60%	80.53%
Coranti 2010		99.83%	99.55%	99.45%	99.61%	94.91%	98.43%
Defenx Security Suite 2011	VIRUS 100	89.49%	88.50%	81.64%	86.54%	76.32%	83.99%
Digital Defender	VIRUS 100	91.13%	85.74%	79.68%	85.52%	75.82%	83.09%
eEye Blink Server	VIRUS 100	93.70%	85.67%	82.34%	87.24%	87.88%	87.40%
Emsisoft Anti-Malware for Server		99.56%	98.03%	97.80%	98.47%	92.63%	97.01%
eScan Internet Security Suite	VIRUS 100	98.32%	97.73%	94.92%	96.99%	88.09%	94.76%
ESET NOD32 Antivirus	VIRUS 100	94.84%	91.96%	95.18%	93.99%	90.51%	93.12%
Fortinet FortiClient	VIRUS 100	96.25%	95.61%	90.35%	94.07%	81.41%	90.90%
Frisk F-PROT Antivirus		75.61%	75.22%	80.06%	76.96%	80.90%	77.95%
F-Secure Protection Service	VIRUS 100	98.51%	98.24%	94.93%	97.23%	88.46%	95.03%
G Data AntiVirus Client		99.68%	99.28%	98.57%	99.18%	93.92%	97.86%
Ikarus virus.utilities		99.41%	97.43%	97.16%	98.00%	91.37%	96.34%
Kaspersky Small Office Security	VIRUS 100	96.86%	94.85%	96.13%	95.95%	89.15%	94.25%
Keniu Antivirus		96.94%	95.11%	95.39%	95.81%	63.68%	87.78%
Kingsoft AntiVirus 2011 Advanced A	VIRUS 100	27.22%	22.27%	22.56%	24.02%	31.84%	25.97%
Kingsoft AntiVirus 2011 Advanced B		45.42%	40.11%	51.89%	45.81%	57.90%	48.83%
Kingsoft AntiVirus 2011 Standard	VIRUS 100	15.60%	11.27%	21.47%	16.11%	21.93%	17.57%
Lumension EMSS *	VIRUS 100	94.90%	91.01%	87.76%	91.22%	31.73%	76.35%
Microsoft Forefront Endpoint Protection 2010	VIRUS 100	93.72%	91.82%	90.47%	92.00%	86.97%	90.75%
Mongoosa	VIRUS 100	74.85%	70.12%	76.41%	73.79%	79.25%	75.16%
Norman Security Suite	VIRUS 100	93.74%	85.71%	82.42%	87.29%	87.97%	87.46%
Preventon Antivirus for Server	VIRUS 100	91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
Quick Heal AntiVirus 2011 Server Ed.	VIRUS 100	94.05%	88.36%	87.77%	90.06%	84.29%	88.62%
Returnil System Safe 2011		78.21%	78.32%	82.99%	79.84%	82.60%	80.53%
Sophos Endpoint Security and Control	VIRUS 100	93.04%	89.04%	90.80%	90.96%	78.76%	87.91%
SPAMfighter VIRUSfighter	VIRUS 100	91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
GFI/Sunbelt VIPRE Antivirus	VIRUS 100	98.25%	95.18%	94.75%	96.06%	87.62%	93.95%
TGSoft VirIT eXplorer PRO		33.79%	22.97%	31.43%	29.40%	26.26%	28.61%
Trustport Antivirus 2011	VIRUS 100	99.87%	99.71%	99.87%	99.81%	94.43%	98.47%
VirusBuster For Windows Server	VIRUS 100	90.98%	86.53%	85.13%	87.54%	80.87%	85.88%

* Repeatedly failed to complete final scan.

(Please refer to text for full product names.)

Testing ran through in good time with no stability problems or unexpected slowdowns, and both scanning speeds and file access lag times were pretty good. Resource use was low and impact on our set of activities likewise minimal.

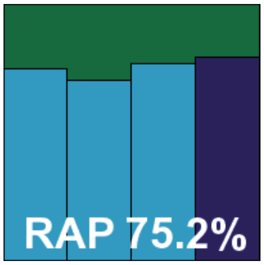
Detection rates were also good, with a slight decline through the RAP sets as expected, and with no problems in the core certification sets, *Microsoft* comfortably earns another VB100 award. *Forefront* is an irregular entrant in our tests, usually alternating with *Microsoft*'s consumer-level offering, but has passed all three entries in the last year; six in the last 12 tests with the other six not entered.

Mongoosa

Version 2.1

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	89.33%
Worms & bots	94.25%	**False positives**	0

vb 100 VIRUS virusbtn.com June 2011



Mongoosa is another new name in the VB100 line-up, but this time we had been able to take a look at the product prior to the test as the developers readied it for full release. *Mongoosa* is a Canadian company whose product provides a fully featured firewall alongside anti-malware protection based on the ubiquitous *VirusBuster* engine. The product was provided as a mid-sized 81MB installer, which is fairly simple and fast to run through, although a web connection is required to apply a licence key. The set-up finishes with a reboot.

The interface is rather stylized but doesn't stray too far from the standard approach, making navigation fairly straightforward after a little exploration. Options are fairly basic, but the main requirements are all covered, and the product seemed fairly stable and responsive throughout testing, even under heavy loads.

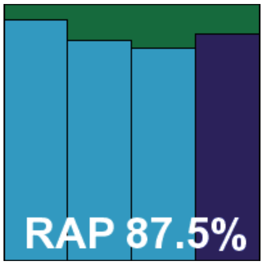
Scanning speeds were not bad, and on-access lags were OK too, with low use of resources and not much effect on our set of standard activities. Detection rates were a little fiddly to extract from the log system – which offers no option to export to plain text – but with some careful processing of raw database files we eventually got a full set of results. These showed some good scores in the main sets, but RAP scores were a little lower than expected for the underlying engine, even after repeat runs, for no obvious reason. Nevertheless, the WildList and clean sets were properly handled, and *Mongoosa* becomes the second new name to be added to the list of VB100 certified solutions this month.

Norman Security Suite

Virus Control version 7.20, Norman Scanner Engine 6.07.07

ItW	100.00%	**Polymorphic**	99.98%
ItW (o/a)	100.00%	**Trojans**	96.06%
Worms & bots	96.33%	**False positives**	0

vb 100 VIRUS virusbtn.com June 2011



Back on more familiar ground, *Norman* is another of our most regular participants, and seems to be recovering after a run of bad luck in our tests. The suite solution came as a rather hefty 441MB installer, which nevertheless got things set up in reasonable time. The product interface is browser-based and not too fiddly to navigate but it suffers from the occasional slow response to clicks and lost connections – as seems to be the norm with such approaches. Configuration is available in reasonable detail for those with the patience to get at it.

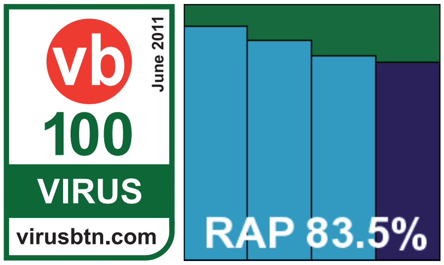
As with other products based on the same engine, getting through the tests took well over a week – a situation not helped by the scheduler system sitting and waiting for input over a long weekend; one would normally expect a scheduled job to operate independently, following pre-set actions rather than stopping and asking for advice on how to proceed at the first sign of danger. Our speed measures show slow scanning speeds and rather heavy lag times when accessing files, with a fair amount of RAM and CPU being consumed, but our set of tasks were completed fairly quickly.

Detection rates were decent, with good coverage of our main sets and reasonable scores in the RAP sets, even improving slightly in the proactive week. The core certification requirements were met without mishap, and *Norman* earns another VB100 award. *Norman*'s recent test history shows five passes and a single fail in the last six tests; six passes and four fails in the last dozen, with two not entered.

Preventon Antivirus for Server

Version: 4.3.56, Definitions date: 18/04/2011, Definitions version: 13.6.31

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.53%
Worms & bots	94.24%	**False positives**	0



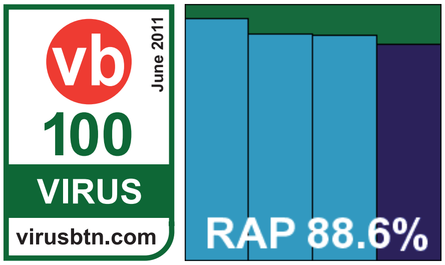
The originator of a number of products already described this month, *Preventon* provided no surprises. The 74MB installer ran through in good time and required online activation and updating, which also seemed fairly fast and painless. The interface is clear and simple, not overloaded with fine-tuning controls but covering the basic bases. Operation seemed reliable with no loss of stability under pressure, and tests completed in good time. Scanning speeds were decent and overheads fairly light, with only CPU use perhaps a little above average.

Detection rates were decent too, with a good showing across the board, and with no issues in the WildList or clean sets *Preventon* comfortably makes the grade for a VB100 award. In the ten tests since its first entry, *Preventon* has amassed two passes and two fails in the last year; four passes and two fails in total.

Quick Heal AntiVirus 2011 – Server Edition

Version: 12.00 (5.0.0.5), SP1

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	96.47%
Worms & bots	97.45%	**False positives**	0



Quick Heal is another regular on our test bench, with a long history of appearances. Its current edition, provided as a 206MB installer, set itself up in good time with only a few clicks and no need to reboot – all of which was done in under a minute. The interface has been jazzed up considerably of late and looks good, going for the row-of-large-buttons approach but providing excellent controls under the glossy covers. Usability is good thanks to a clear and logical layout.

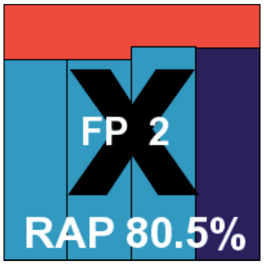
Stability was also good, and tests completed in reasonable time, with zippy scanning speeds and low lag times in the standard file access measures. RAM use was a little high, but processor drain was not excessive. Running through our suite of standard activities was a whole other story though. This took an extraordinarily long time to complete – so much outside the expected bounds that we re-ran the test several times. Despite testing on different systems with fresh installs, each test run showed the same thing: the set of tasks took 20 times longer than the baseline measures. Watching the progress, it appeared that the bulk of the delay was in the downloading of *Office* documents from our local web server, with the later local manipulation of the same files running through at much more reasonable speed.

Detection tests threw up fewer surprises though, taking a little time to get through but nothing excessive, and when the results were parsed there were some pretty decent scores – a little better on demand than on access, as we usually see from this product. The certification sets were properly handled and a VB100 award is duly earned. *Quick Heal*'s recent history is exemplary, with six passes in the last six tests; 11 passes and a single fail in the last two years – the vendor last missed a comparative in November 2003.

Returnil System Safe 2011

Version 4.2.12471.5765-REL13

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	78.88%
Worms & bots	84.01%	**False positives**	2



Returnil's unique selling point is a virtualization system enabling rollback of any changes to the protected machine at the click of a button; the additional anti-malware component is provided by the *Frisk* engine. The installer is a compact 33MB, accompanied by a 60MB update bundle. The install process is fast and simple, with the full details of the EULA tucked away in an 'advanced' section. Installation is complete in half a minute, but a reboot is needed to fully activate all features.

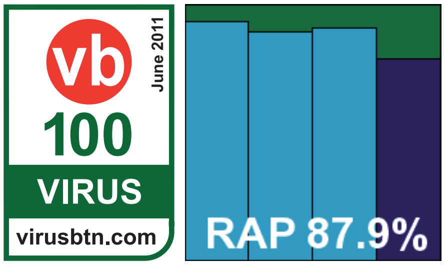
The interface is bright and cheerful, with a sensible, straightforward layout making for good usability. The look and feel is very much geared towards the consumer end of the market, but it seemed to run smoothly and stably on this month's server platform. Scanning speeds were a little slow and on-access overheads higher than some, and both resource use and impact on our set of tasks were a little high too.

Detection rates were no more than reasonable, but coverage was fairly reliable across the sets, with no major peaks or troughs. The WildList was handled smoothly, but as expected, the pair of items in the clean sets which have tripped up others using the same engine reappeared, denying *Returnil* a VB100 award this month. *Returnil* remains on three passes since its first entry a year ago, with two fails and no entry in the *Linux* test.

Sophos Endpoint Security and Control

Sophos Anti-Virus 9.7.0, Detection engine 3.18.27, Detection data 4.64G

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	87.93%
Worms & bots	96.80%	**False positives**	0



Sophos is a business-focused firm and its solutions are appropriately businesslike. The 80MB installer is supplemented by a svelte 7MB offline update bundle, and the set-up process is simple and speedy. A rejig of the company's branding provides a new splash screen at the start, with a colour-drained 'S' resembling a pallid Superman logo, but the remainder of the process remains unaffected. The whole job was done in good time, with no need to reboot at the end.

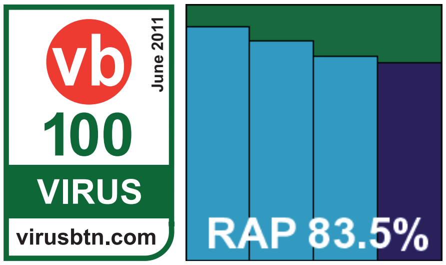
The interface also remains unchanged by the rebranding, keeping its stark and plain styling, with good usability and extreme depth of configuration available to those willing to meddle with the fine settings. Testing in general was pretty stable, although in the RAP sets some samples seemed to snag the scanner somewhat, in some cases leaving it stuck on the same file indefinitely. On closer inspection these appeared to be malformed items not removed by our basic filtering process before testing commenced. The more real-world tests ran well, with fast scanning speeds and low lag times. The resource consumption and activity measures also showed very low impact.

Detection rates were splendid, with solid scores across the sets, declining slightly through the RAP sets. The core certification sets were dealt with ably, and *Sophos* comfortably earns another VB100 award. The last year has been solid for *Sophos*, with six passes out of six entries; over two years the company has 11 passes and a single fail.

SPAMfighter VIRUSfighter

Version: 7.0.214

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	86.53%
Worms & bots	94.24%	**False positives**	0



Another product based on the *Preventon* SDK, but with a little more of the company's own efforts having gone into the GUI design, *SPAMfighter*'s solution was another 74MB installer which skipped through a few quick steps and was up and running in under a minute with no need to reboot. The interface has seen some small tweaks since we last tested it, with some confusing options rendered more obvious, and tests ran through simply and easily. The only problem we encountered was the lack of an option to prevent logs from being deleted after reaching a certain size – but we got around the problem by splitting larger tests into multiple jobs.

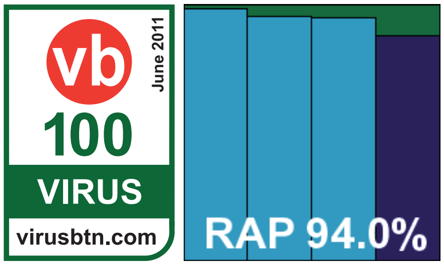
Speeds and overheads were reasonable, if not overly exciting, and RAM use and impact on our set of tasks were both fairly low, although CPU use was a little on the high side. Detection rates were respectable, with decent scores across the board and there were no problems meeting the core requirements. *SPAMfighter* thus earns a VB100 award, its tally now standing at two passes and two fails in the last year; three passes and three fails since it first entered eight tests ago.

GFI/Sunbelt VIPRE Antivirus

Version 4.0.3904, Definitions version 9077

ItW	100.00%	**Polymorphic**	99.79%
ItW (o/a)	100.00%	**Trojans**	96.81%
Worms & bots	98.66%	**False positives**	0

VIPRE has become an increasingly regular participant in our tests of late, and seems to be steadily improving after some rocky results a few years back. The install process

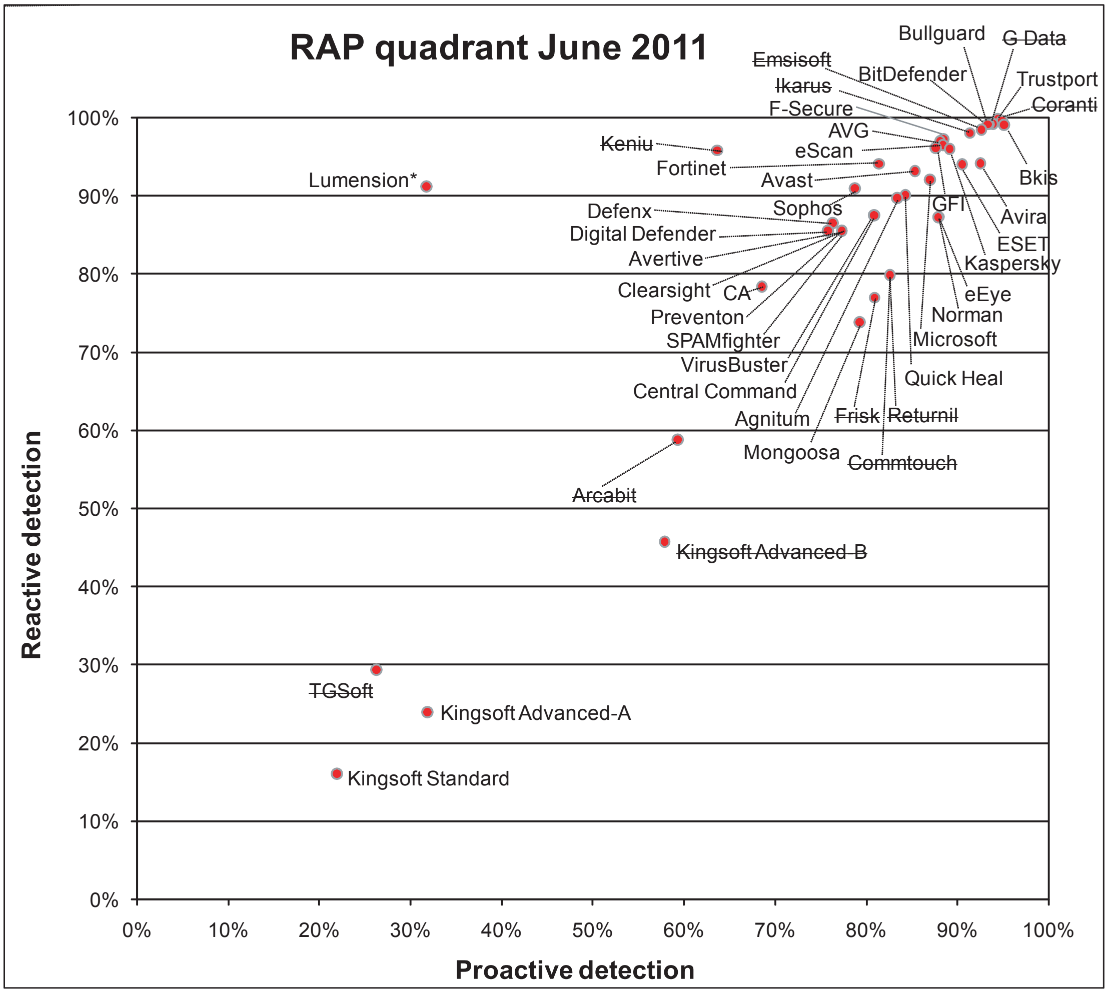


is very rapid, although it does need a reboot, and applying updates is similarly painless. The interface is emblazoned with a large snake emblem which takes up one corner of the GUI, but is otherwise fairly businesslike and straightforward. Options are fairly limited, but cover the main bases, and are for the most part easy to access and operate.

Scanning speeds were distinctly slow, but overheads were not too bad, especially on repeat runs where some smart optimization was clearly in operation. Our suite of activities completed very rapidly, while RAM use was about average and CPU use perhaps a shade higher than most.

The detection tests were a little difficult, thanks to some lingering wobbliness in the scanner; on a few occasions large scans, having run for a day or more, came to a clunking halt with a message reporting 'your scan has failed', and there had been no logging of what had been covered up to that point. However, by re-running jobs we eventually got a full set of figures. These showed some excellent detection rates with impressive scores across the sets. The WildList and clean sets were well managed, earning *VIPRE* another VB100 award.

GFI's record shows four passes and two non-entries in the last year; five passes and a single fail since its first entry ten tests back.



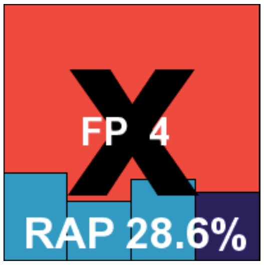
** Product did not finish final scan properly.*

(Products with strikethrough generated false positives. Please refer to text for full product names.)

TGSoft VirIT eXplorer PRO

Version 6.8.87

ItW	62.88%	**Polymorphic**	63.76%
ItW (o/a)	62.52%	**Trojans**	25.33%
Worms & bots	46.49%	**False positives**	4



The third newcomer in this month's test felt like something of a blast from the past. First contacting us shortly before the test deadline, the Italian company was previously unknown to us but appears to have been around for a while. Installing the product hinted at some history, with the release notes claiming continued support for MS-DOS and *Windows 3.x*, long since dropped by most vendors. After a fairly fast set-up process a reboot is needed, and once up the product interface also reflects some great seniority, with a very old-school design. Perhaps thanks to long forgotten muscle memory, the quirky-looking layout proved perfectly simple to navigate and operate, and seemed to run fairly smoothly during our initial tests.

Scanning speeds were super-fast and overheads very low, with very little use of resources or impact on our set of tasks. The interface has an *Explorer*-style tree structure in the left pane, which expands and contracts during scanning to show the folder currently being worked on; at the zippy speeds at which the scans of our clean sets ran, this became quite hypnotic.

Moving onto the infected sets, we hit a small snag when the scanner crashed during the RAP tests, but a retry completed without the problem reappearing. In the on-access test, things were a little more rocky, with a blue screen bringing the system to an abrupt halt; again, a repeat run handled things much better. These issues seem to be due to overwork, occurring only when handling large numbers of detections in short periods, and are thus unlikely to affect real-world users.

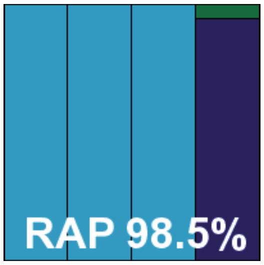
Unfortunately, detection scores were well below par, with a reasonable showing over polymorphic viruses on demand dropping noticeably on access, and fairly low coverage in the trojans and RAP sets. The WildList set showed a fair number of misses – again more on access than on demand – and there were a handful of false alarms in the clean sets too. *TGSoft* doesn't make the grade for VB100 certification this month, but has put in a reasonably good start and should be able to improve rapidly.

Trustport Antivirus 2011

Version 2011 (11.0.0.4614)

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	99.74%
Worms & bots	99.99%	**False positives**	0

vb
June 2011
100
VIRUS
virusbtn.com



Another multi-engine product, *Trustport*'s installer is not too enormous at just under 200MB, and runs through at a reasonable speed with no tricky questions. The layout of the interface is a little unusual, taking a little exploration before the system of mini-interfaces can be deciphered, but with a little practice it soon makes sense and provides a very good level of controls.

Testing was not interrupted by any problems and got through in good time, although scanning speeds were predictably a little slower than most, and overheads and resource usage a little heavier – but nothing seemed too extreme. This slight added weight was more than made up for by the detection scores, which were pretty hard to fault, the product barely missing anything across all the sets and demolishing even the RAP 'week +1' set.

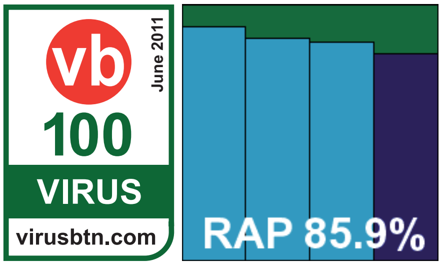
The WildList was handled well, as was the clean set, and *Trustport* earns a VB100 award with some style. All four entries in the last year have earned *Trustport* a pass, and the vendor has had no fails from nine entries in the last 12 tests.

VirusBuster For Windows Server

Product version 7.1.52, engine 5.2.0, database 13.6.313

ItW	100.00%	**Polymorphic**	100.00%
ItW (o/a)	100.00%	**Trojans**	91.34%
Worms & bots	79.22%	**False positives**	0

VirusBuster's server product has already been tested this month in another guise, and the engine has been put through its paces in a number of shapes and sizes. This original version came in as a 66MB installer with 68MB of updates, and again hid the option to join a feedback scheme on the EULA page. The set-up process was fairly fast though, completing with a reboot. The MMC interface is a little fiddly, with plenty of room for confusion and misunderstanding, but provides a decent level of controls for those willing to wrestle them into shape.



Scanning speeds and overheads were unexceptional – around the middle of the pack in most areas – with a slightly heavier than average impact on our set of activities. Stability was good though, and scan times through the infected sets not too bad after some serious sluggishness in the last test. Final results showed the expected decent detection rates, no problems in the WildList or clean sets, earning *VirusBuster* another VB100 award. The vendor has passed all of the last six tests, with nine passes and three fails in the last year, and has skipped only two tests since its first entry over a decade ago.

CONCLUSIONS

While the majority of products performed well this month, remaining steady under heavy fire and producing clear, easy to follow reports, some were unruly and uncooperative, requiring serious effort to operate. Once again a small group of products dominated lab time, with a handful taking several weeks to complete some of the bigger jobs. In future it may become necessary to impose time limits on all of our tests in the same way as we have done on the speed measures – a move which proved its worth this month despite having set what we originally thought was a very high limit.

These irritations aside, it was a good month in general, with some excellent detection rates and a high pass ratio. Of those not quite making the grade, the majority were tripped up by small numbers of false alarms, which can happen to the best of products; indeed, some of those not qualifying for awards this month put in truly excellent performances. As always, we advise readers to take a longer-term view, monitoring the performance of solutions (and vendors) over longer periods to get a true picture of their reliability.

Some expansions to the tests we had hoped to add this month have had to be delayed due to the unforeseen problems, but we hope in the near future to broaden the range of tests we can report on. As always, we welcome feedback and suggestions from our readers on any aspect of the tests.

Technical details

All products were tested on identical machines with *AMD Phenom II X2* 550 processors, 4 GB RAM, dual 80GB and 1TB hard drives, running *Windows Server 2008 R2*, *Enterprise Edition, Service Pack 1*. For full testing methodology see http://www.virusbtn.com/vb100/about/methodology.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 Web: http://www.virusbtn.com/