

# virus

## BULLETIN

### EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS FEBRUARY – JUNE 2011

#### VIRUS BULLETIN VB100 TESTING

The basic requirements for a product to achieve VB100 certification status are that a product detects, both on demand and on access, in its default settings, all malware known to be 'In the Wild' at the time of the review, and generates no false positives when scanning a set of clean files.

Various other tests are also carried out as part of the comparative review process, including speed and overhead measurements and 'RAP' (Reactive and Proactive) tests.

The RAP tests measure products' detection rates across four distinct sets of malware samples. The first three of these comprise malware first seen in each of the three weeks prior to product submission and measure how quickly product developers and labs react to the steady flood of new malware. The fourth test set consists of malware samples first seen in the week after product submission. This test set is used to gauge products' ability to detect new and unknown samples proactively, using heuristic and generic techniques.

While the results of these secondary tests do not affect a product's qualification for VB100 certification, they are included to provide the reader with a better overall picture of product performance.

The testing methods of the VB100 certification process are provided in more detail at <http://www.virusbtn.com/vb100/about/100procedure.xml>.



#### FEBRUARY 2011: UBUNTU LINUX 10.04 LTS

This test was run on the explosively popular *Ubuntu* distribution, which was first seen on the VB100 test bench in June 2008. The main issue we expected to see was with on-access scanning, which is always slightly fiddly on *Linux*. In the past there have been three main approaches: protecting *Samba* shares only, using *Samba* vfs objects, which usually entails little more than an added line or two in the *Samba* configuration file; the open-source *dazuko* system, which allows more granular control of protection over different areas of the system; and proprietary methods, which can vary greatly from provider to provider.












The latest WildList available on the deadline date was the November 2010 list, released in late December. This was used to compile the core certification set and featured mainly standard worms and online gaming password-stealers. With several older file infectors removed from the list it shrank to a little over 5,000 samples, the bulk of which were from two remaining file infectors, a single strain of W32/Virut and the venerable W32/Polip.

#### ESET File Security 3.0.20

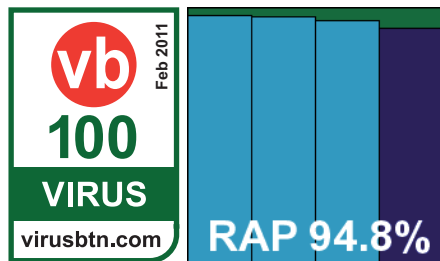
<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	94.18%
<b>Worms &amp; bots</b>	98.62%	<b>False positives</b>	0

*ESET's Linux* edition was provided as a single 41MB .DEB package, and installed easily with minimal fuss. Clear instructions showed how to set up protection of *Samba* shares using a vfs object (*dazuko*-style protection was also



Reactive And Proactive (RAP) scores February 2011		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Avast		92.27%	98.25%	95.98%	95.50%	82.55%	92.26%
AVG		97.13%	97.11%	88.86%	94.37%	78.07%	90.29%
Avira		99.71%	99.72%	96.05%	98.49%	93.55%	97.26%
BitDefender		98.76%	99.38%	99.01%	99.05%	92.10%	97.31%
Central Command		88.69%	90.68%	85.35%	88.24%	83.64%	87.09%
eScan		97.21%	95.98%	94.12%	95.77%	87.10%	93.60%
ESET		96.53%	96.34%	94.89%	95.92%	91.51%	94.82%
Frisk		80.83%	75.41%	62.50%	72.91%	76.00%	73.69%
Kaspersky AV		91.32%	90.54%	86.68%	89.51%	85.37%	88.48%
Kaspersky ES		92.41%	92.08%	86.71%	90.40%	83.25%	88.61%
Norman		66.49%	61.56%	62.78%	63.61%	59.48%	62.58%
Quick Heal		92.43%	85.20%	76.69%	84.78%	82.07%	84.10%
Sophos		91.46%	90.81%	92.84%	91.71%	87.72%	90.71%
VirusBuster		88.69%	90.68%	85.35%	88.24%	83.64%	87.09%

available), and the commands and configuration were properly laid out, conforming to expected norms.



Running the test was fairly painless, although a couple of files in our extended sample sets did cause segmentation faults and required the restarting of scans. Speeds were pretty zippy and overheads nice and light, particularly in the binaries section. Detection rates were solid across the sets. The clean set threw up a few warnings of potentially unwanted items (most identified precisely and accurately) and a couple of packer warnings, but nothing could stop ESET's inexorable progress towards yet another VB100 award.




























### APRIL 2011: WINDOWS XP SP3

































When *Windows XP* first came out, George W. Bush was still in his first year of presidency. The 9/11 attacks took place between the platform's release to manufacture and going on retail sale, as did the launch of the first generation

*iPod*. *Wikipedia* was less than a year old, *Google* was just starting to turn a profit, while the likes of *Facebook*, *Skype*, *YouTube* and *World of Warcraft* were yet to come. Skip forward almost a decade, and *XP* is still with us – not just hanging on by its fingertips but firmly remaining the most popular desktop platform (some estimates put it on over half of all desktop systems, and most agree that it runs on at least 40%). It is familiar, cheap, (comparatively) reliable and very popular. To most of the world's computer users, it's just the way computers work.

The WildList set was synchronized with the January 2011 issue of the WildList. This meant a few new additions to the core certification set, the bulk of which were simple autorun worms and the like. Most interesting to us were a pair of new W32/Virut strains, which promised to tax the products, and as usual our automated replication system churned out several thousand confirmed working samples to add into the mix.

The deadline for product submission was 23 February, and as usual our RAP sets were built around that date, with three sets compiled from samples first seen in each of the three weeks before that date, and a fourth set from samples seen in the week that followed. In total, after verification and classification to exclude less prevalent items, we included a weekly average of 20,000 samples in the RAP sets.

Reactive And Proactive (RAP) scores April 2011		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		91.40%	93.24%	87.51%	90.72%	83.08%	88.81%
AhnLab V3 Internet Security		94.44%	94.15%	82.34%	90.31%	82.37%	88.32%
Antiy Ghostbusters		59.95%	65.11%	56.99%	60.68%	65.88%	61.98%
ArcaBit ArcaVir		66.29%	65.23%	57.16%	62.89%	56.73%	61.35%
AvailaSoft AS Anti-Virus		40.46%	42.15%	39.69%	40.77%	51.76%	43.52%
Avast Software avast! Free		98.29%	97.74%	95.03%	97.02%	90.02%	95.27%
Avertive VirusTect		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
AVG Internet Security		95.11%	95.95%	94.75%	95.27%	84.38%	92.55%
Avira AntiVir Personal		98.40%	98.82%	95.69%	97.64%	91.21%	96.03%
Avira AntiVir Professional		98.40%	98.82%	95.69%	97.64%	91.21%	96.03%
BitDefender Antivirus Pro		97.55%	95.45%	92.33%	95.11%	89.28%	93.65%
Bkis BKAV Professional		97.93%	96.56%	95.17%	96.55%	92.15%	95.45%
Bullguard Antivirus		98.48%	98.47%	96.06%	97.67%	91.61%	96.15%
CA Internet Security Suite Plus		79.60%	79.31%	77.01%	78.64%	77.06%	78.25%
CA Total Defense r12		77.33%	74.81%	71.90%	74.68%	73.68%	74.43%
Central Command Vexira		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Check Point Zone Alarm		95.71%	95.23%	94.31%	95.08%	90.79%	94.01%
Clearsight Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
CommTouch Command		84.14%	74.95%	71.80%	76.97%	79.72%	77.66%
Comodo I.S. Premium		90.21%	90.19%	80.33%	86.91%	78.33%	84.77%
Coranti 2010		99.70%	99.76%	97.97%	99.14%	93.30%	97.68%
Defenx Security Suite		91.22%	93.00%	87.53%	90.59%	82.95%	88.68%
Digital Defender		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
eEye Blink		84.70%	85.02%	75.86%	81.86%	79.57%	81.29%
EmsiSoft Anti-Malware		95.72%	95.22%	90.18%	93.71%	86.77%	91.97%
eScan Internet Security		98.71%	99.06%	95.84%	97.87%	91.67%	96.32%
ESET NOD32		94.24%	94.31%	94.92%	94.49%	89.86%	93.33%
Filseclab Twister		67.63%	73.88%	70.22%	70.58%	76.41%	72.03%
Fortinet FortiClient		94.12%	95.34%	84.59%	91.35%	78.53%	88.15%
Frisk F-PROT		82.53%	72.59%	67.67%	74.26%	76.76%	74.89%
F-Secure Client Security		98.46%	98.78%	94.60%	97.28%	91.43%	95.82%
F-Secure Internet Security		98.53%	98.84%	94.69%	97.35%	91.50%	95.89%
G DATA AntiVirus 2011		99.94%	99.82%	95.88%	98.55%	92.17%	96.95%
Hauri ViRobot Desktop		65.26%	69.24%	62.33%	65.61%	74.07%	67.73%
Ikarus T3 virus.utilities		98.50%	99.48%	98.72%	98.90%	91.84%	97.13%

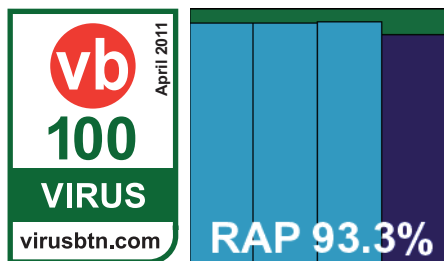
Reactive And Proactive (RAP) scores April 2011 contd.		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
iolo System Shield		76.12%	72.43%	67.46%	72.01%	76.97%	73.25%
K7 Total Security		86.13%	78.12%	75.25%	79.83%	82.20%	80.42%
Kaspersky Anti-Virus 6		95.50%	95.20%	93.18%	94.63%	89.32%	93.30%
Kaspersky Internet Security		96.42%	95.67%	94.99%	95.69%	91.17%	94.56%
Kaspersky PURE		96.39%	95.64%	94.96%	95.66%	91.18%	94.54%
Keniu Antivirus		96.44%	95.69%	94.60%	95.58%	90.78%	94.38%
Keyguard Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
Kingsoft I.S. 2011 Advanced		24.24%	33.85%	25.46%	27.85%	34.63%	29.54%
Kingsoft I.S. 2011 Standard-A		15.86%	16.54%	13.87%	15.42%	25.52%	17.95%
Kingsoft I.S. 2011 Standard-B		15.86%	16.53%	13.86%	15.42%	25.51%	17.94%
Lavasoft Ad-Aware Total Security		99.95%	99.83%	95.96%	98.58%	92.22%	96.99%
Logic Ocean GProtect		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
McAfee VirusScan Enterprise		86.13%	86.31%	82.73%	85.05%	83.69%	84.71%
Microsoft Forefront Endpoint Protection		94.38%	95.07%	91.12%	93.52%	87.18%	91.94%
Nifty Corp. Security 24		96.39%	95.66%	93.87%	95.30%	90.50%	94.10%
Norman Security Suite		84.72%	85.04%	75.89%	81.88%	79.58%	81.30%
Optenet Security Suite		81.29%	85.30%	79.04%	81.87%	81.48%	81.78%
PC Booster AV Booster		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
PC Renew I.S 2011		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
PC Tools I.S. 2011		94.28%	96.82%	87.04%	92.72%	83.00%	90.29%
PC Tools Spyware Doctor		94.28%	96.82%	87.04%	92.72%	83.00%	90.29%
Preventon Antivirus		89.45%	88.91%	82.71%	87.02%	79.86%	85.23%
Qihoo 360 Antivirus		98.86%	98.62%	92.02%	96.50%	90.42%	94.98%
Quick Heal Total Security 2011		92.12%	90.84%	88.37%	90.44%	89.67%	90.25%
Returnil System Safe 2011		85.19%	75.87%	72.61%	77.89%	80.02%	78.42%
Sofscan Professional		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Sophos Endpoint Security and Control		91.34%	93.16%	88.46%	90.99%	83.59%	89.14%
SPAMfighter VIRUSfighter		89.28%	88.46%	80.62%	86.12%	78.68%	84.26%
GFI/Sunbelt VIPRE		98.67%	99.35%	95.59%	97.87%	84.66%	94.57%
Symantec Endpoint Protection		92.92%	95.82%	84.06%	90.94%	81.50%	88.58%
Trustport Antivirus 2011		99.82%	99.86%	99.21%	99.63%	93.18%	98.02%
UnThreat Antivirus Professional		98.67%	99.36%	95.59%	97.87%	84.66%	94.57%
VirusBuster Professional		91.86%	93.50%	87.90%	91.09%	83.17%	89.11%
Webroot Internet Security Complete		91.92%	93.53%	87.84%	91.10%	83.70%	89.25%

## ESET NOD32 Antivirus 4

Version 4.2.71.2; virus signature database: 5901  
(20110223)

<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	89.29%
<b>Worms &amp; bots</b>	98.13%	<b>False positives</b>	0

*ESET* has an illustrious history in our tests, still holding onto its record for the longest unbroken run of certification passes – and indeed comparatives taken part in, the vendor not having missed a test since 2003.



The current product has been in stable form for some time. This month's submission, a nice small 44MB executable, was installed with the standard steps, enlivened as usual by the enforced choice of whether or not to detect 'potentially unwanted' software – the 'next' button is greyed out until a selection is made. It doesn't take long and no reboot is needed, just a short pause before the protection is in place.

The interface is simple and unfussy, but provides a wealth of fine-tuning controls. There is so much here that some of it seems to be a little superfluous and in places overlapping, and we have long had trouble figuring out the controls for scanning inside archives on access. However, it is generally solid and intuitive. Occasionally the interface tends to get itself in a bit of a twist after a scan job, but it invariably sorts itself out within a few moments, and the only other issue noted was the occasional scan display screen not finishing properly, lingering at 99% when logs showed the scan had already completed without problems.

Scanning speeds were OK, and on-access lag times fairly low too, with low use of resources. Impact on our set of activities was a little higher than most, but not too much.

Detection rates were excellent as usual, with most of the sets demolished and there was superb regularity in the reactive part of the RAP sets. A couple of items were flagged as unsavoury in the clean sets, one of them being packed with Themida and another a toolbar, but no problems arose there or in the WildList – thus earning *ESET* yet another VB100 award to maintain the 100% record it has held for the best part of a decade.

## JUNE 2011: WINDOWS SERVER 2008 R2

Our platform this time 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. 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.

The February 2011 WildList 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 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.

## ESET NOD32 Antivirus 4

Version 4.2.72.0, Virus signature database 6058  
(20110420)

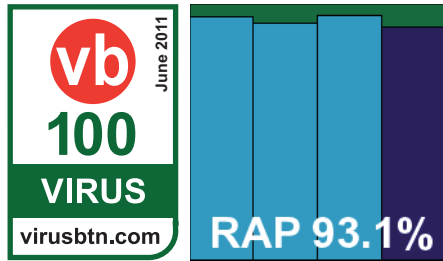
<b>ItW</b>	100.00%	<b>Polymorphic</b>	99.99%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	94.38%
<b>Worms &amp; bots</b>	96.35%	<b>False positives</b>	0

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

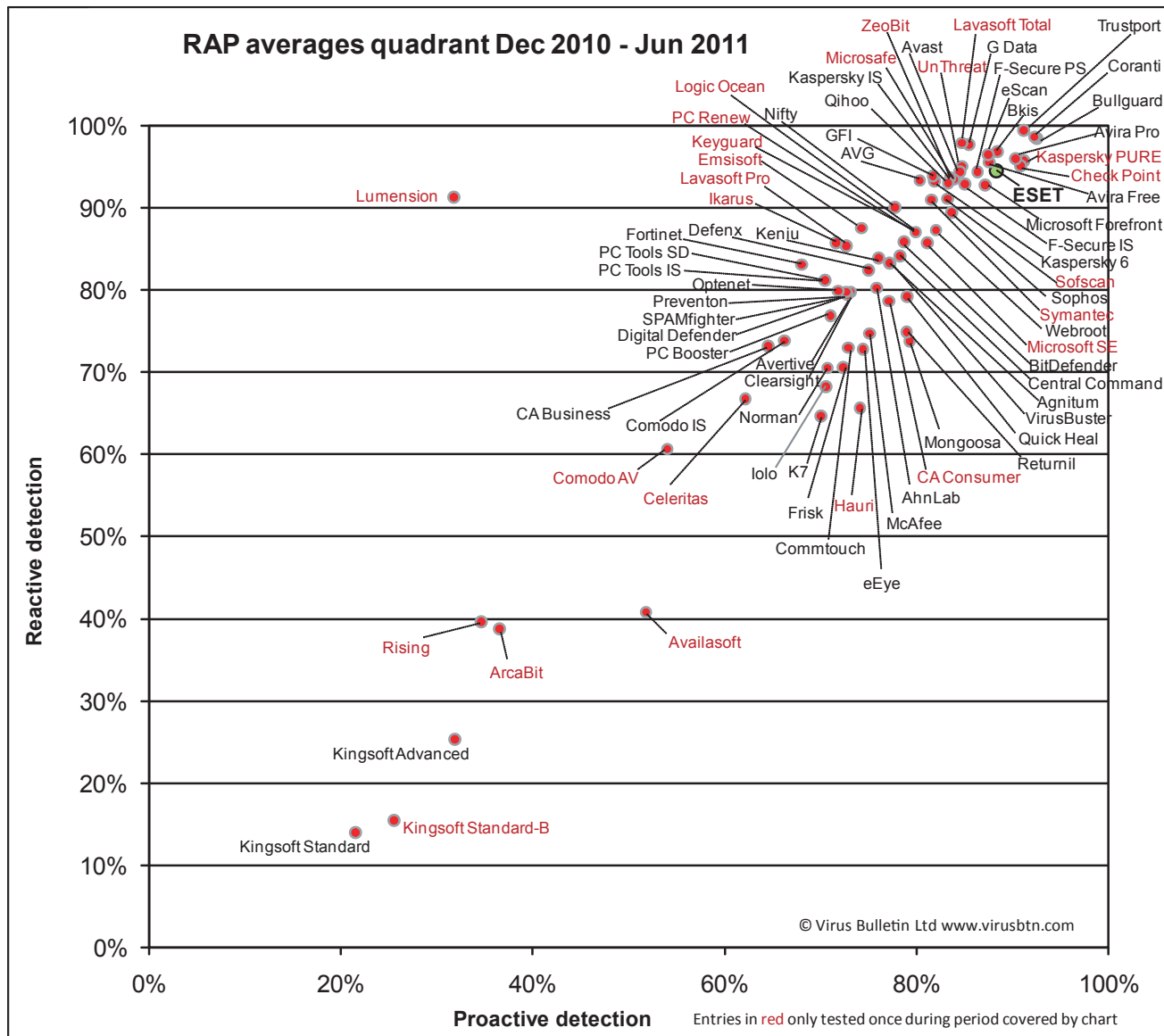
some solid coverage of the sets, no problems in the core certification sets, and ESET once again earns a VB100 award. The vendor's record is exemplary, with all of the last 12 tests (indeed, all of the last 47 tests) entered and passed.



































ESET, 610 West Ash St, Suite 1900,  
San Diego, CA 92101, USA

Tel: +1 619 876 5400, Fax: +1 619 437 7045

Email: sales@eset.com, Web: http://www.eset.com/.



Reactive And Proactive (RAP) scores June 2011		Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost Security Suite Pro		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		96.89%	92.88%	89.71%	93.16%	85.36%	91.21%
Avertive VirusTect		91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
AVG Internet Security 2011		97.50%	96.65%	95.20%	96.45%	88.41%	94.44%
Avira AntiVir Server		99.13%	87.60%	95.65%	94.12%	92.52%	93.72%
BitDefender Security for File Servers		99.37%	99.04%	98.91%	99.11%	93.32%	97.66%
Bkis BKAV Professional I.S.		99.46%	98.78%	99.03%	99.09%	95.13%	98.10%
Bullguard AntiVirus		99.37%	99.04%	98.97%	99.13%	93.39%	97.69%
CA Total Defense r12 I.S.		85.59%	76.81%	72.88%	78.42%	68.55%	75.96%
Central Command Vexira		90.97%	86.46%	85.13%	87.52%	80.84%	85.85%
Clearsight Antivirus		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		89.49%	88.50%	81.64%	86.54%	76.32%	83.99%
Digital Defender		91.13%	85.74%	79.68%	85.52%	75.82%	83.09%
eEye Blink Server		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		98.32%	97.73%	94.92%	96.99%	88.09%	94.76%
ESET NOD32 Antivirus		94.84%	91.96%	95.18%	93.99%	90.51%	93.12%
Fortinet FortiClient		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		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		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		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		15.60%	11.27%	21.47%	16.11%	21.93%	17.57%
Lumension EMSS *		94.90%	91.01%	87.76%	91.22%	31.73%	76.35%
Microsoft Forefront Endpoint Protection 2010		93.72%	91.82%	90.47%	92.00%	86.97%	90.75%
Mongoosa		74.85%	70.12%	76.41%	73.79%	79.25%	75.16%
Norman Security Suite		93.74%	85.71%	82.42%	87.29%	87.97%	87.46%
Prevention Antivirus for Server		91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
Quick Heal AntiVirus 2011 Server Ed.		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		93.04%	89.04%	90.80%	90.96%	78.76%	87.91%
SPAMfighter VIRUSfighter		91.13%	85.74%	79.68%	85.52%	77.32%	83.47%
GFI/Sunbelt VIPRE Antivirus		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		99.87%	99.71%	99.87%	99.81%	94.43%	98.47%
VirusBuster For Windows Server		90.98%	86.53%	85.13%	87.54%	80.87%	85.88%

\* Repeatedly failed to complete final scan.