

# virus

## BULLETIN

### EXCERPTS FROM VIRUS BULLETIN COMPARATIVE REVIEWS AUGUST – DECEMBER 2011

#### VIRUS BULLETIN VB100 TESTING

The basic requirements for a product to achieve VB100 certification status are that a product detects, 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>.



#### AUGUST 2011: WINDOWS VISTA X64

*Vista* has been plagued by criticisms and complaints since its first appearance in 2007, and has quickly been superseded by a far superior replacement in *Windows 7*. Usage of *Vista* has declined very gradually though, with latest estimates putting it on around 10% to 15% of desktops. This makes it still a pretty significant player in the market, and we feel obliged to continue checking how well the current crop of anti-malware solutions perform on the platform.

The clean test set saw a fair bit of attention this month, with the usual cleanup of older and less relevant items, and the addition of a swathe of new files culled from magazine cover CDs, the most popular items from major download sites, as well as items from the download areas of some leading software brands. The final set weighed in at just over half a million files, 140GB.

The WildList set included nothing too remarkable, with several variants of W32/Virut falling off the list, leaving very few complex polymorphic items remaining.



















#### ESET NOD32 Antivirus 4

Version 4.2.71.2, Virus signature database 6229

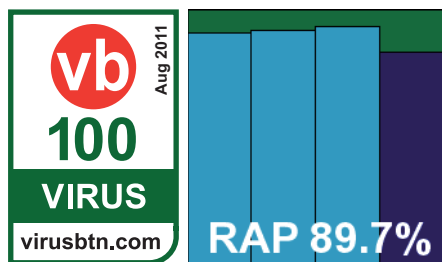
<b>ItW</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>ItW (o/a)</b>	100.00%	<b>Trojans</b>	95.36%
<b>Worms &amp; bots</b>	96.70%	<b>False positives</b>	0

Still maintaining the record for the longest run of passes, *ESET* is one of our most regular participants. The latest product version was provided as a fairly small 51MB package, including all required updates, and installed in



Reactive And Proactive (RAP) scores August 2011	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		86.18%	81.42%	75.04%	80.88%	67.99%	77.66%
AhnLab Internet Security		90.85%	84.31%	81.39%	85.52%	71.10%	81.91%
Avast Software avast! Free Antivirus		97.83%	97.80%	93.45%	96.36%	81.68%	92.69%
AVG Internet Security		95.60%	95.83%	92.34%	94.59%	76.37%	90.03%
Avira AntiVir Personal		97.84%	95.77%	93.83%	95.81%	85.43%	93.22%
Avira AntiVir Professional		97.84%	95.77%	93.83%	95.81%	85.43%	93.22%
BitDefender Security for File Servers		95.11%	92.91%	93.81%	93.94%	81.92%	90.94%
BullGuard Antivirus		98.25%	97.69%	96.97%	97.64%	86.55%	94.87%
Central Command Vexira		86.20%	81.47%	74.93%	80.87%	67.92%	77.63%
Clearsight Antivirus		81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
Commtouch Command Anti-Malware		70.89%	61.99%	66.21%	66.36%	66.72%	66.45%
Comodo Antivirus		90.55%	66.32%	64.51%	73.79%	46.65%	67.01%
Comodo Internet Security PREMIUM		90.55%	66.32%	64.51%	73.79%	46.65%	67.01%
Defenx Security Suite 2011		85.80%	76.26%	72.47%	78.17%	67.78%	75.57%
Digital Defender Antivirus Pro		81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
eEye Digital Security Blink Professional		91.19%	77.46%	74.25%	80.97%	69.13%	78.01%
Emsisoft Anti-Malware		99.66%	99.39%	96.84%	98.63%	84.68%	95.14%
eScan Internet Security Suite		98.23%	97.64%	95.82%	97.23%	85.35%	94.26%
ESET NOD32 Antivirus		90.82%	91.58%	93.25%	91.88%	83.24%	89.72%
Fortinet FortiClient		96.34%	93.82%	92.45%	94.20%	79.63%	90.56%
Frisk F-PROT Antivirus for Windows		69.89%	61.54%	65.52%	65.65%	65.81%	65.69%
F-Secure Client Security		77.53%	72.57%	76.57%	75.56%	68.99%	73.91%
G Data AntiVirus 2012		99.70%	99.71%	95.54%	98.32%	88.46%	95.85%
GFI VIPRE Antivirus		96.83%	95.77%	91.89%	94.83%	79.03%	90.88%

a handful of standard steps, enlivened only by the usual step of forcing a decision on whether or not to detect 'potentially unwanted' items. The process doesn't take long, and needs no reboot to finish.






















The interface is attractive and elegant, glossy without losing a sense of solid quality. Configuration is provided in massive depth and is generally easy to navigate if seeming a little repetitive in places. Operation was pretty straightforward, with no problems with stability. Scanning speeds were pretty fast and very consistent, while on-access overheads

were light, resource consumption average and impact on our activities not too heavy.

Detection rates were decent, with again impressive consistency across the weeks of the RAP sets. The clean sets did throw up a fair number of alerts – mostly for toolbars and adware bundled with freeware packages, but also several items from a suite of system cleaning and optimization tools were labelled as potentially unwanted (the same items having been described by another vendor as having 'dubious usefulness').

None of these could be described as a false alarm though, as the descriptions were pretty accurate, and with the WildList handled well ESET comfortably maintains its unbroken record of VB100 passes, having entered and passed every test since the summer of 2003.

With no crashes or other problems of any sort, and good speeds, all tests were comfortably completed within 24 hours.

Reactive And Proactive (RAP) scores August 2011 contd.	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Ikarus virus.utilities		99.60%	99.31%	96.68%	98.53%	84.42%	95.00%
Iolo System Shield		63.83%	56.18%	60.65%	60.22%	58.42%	59.77%
Kaspersky Internet Security 2012		92.66%	92.84%	89.50%	91.67%	80.65%	88.91%
Kaspersky Small Office Security 2		92.87%	93.28%	89.96%	92.04%	81.14%	89.31%
Lavasoft Ad-Aware Total Security		96.39%	94.59%	93.02%	94.66%	81.53%	91.38%
LogicOcean Gprotect		81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
McAfee VirusScan Enterprise		93.46%	82.30%	85.15%	86.97%	76.16%	84.27%
Microsoft Security Essentials		84.38%	85.95%	71.19%	80.51%	67.26%	77.19%
Norman Security Suite		91.27%	77.55%	74.30%	81.04%	69.17%	78.07%
PC Booster AV Booster		81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
PC Tools Internet Security		92.11%	87.18%	83.03%	87.44%	74.33%	84.16%
PC Tools Spyware Doctor with AntiVirus		92.12%	87.40%	83.04%	87.52%	74.34%	84.22%
Preventon		81.42%	70.08%	69.35%	73.62%	64.16%	71.25%
Qihoo 360 Antivirus		98.31%	97.65%	95.05%	97.01%	85.20%	94.06%
Quick Heal Antivirus Pro 2011		78.64%	55.75%	70.04%	68.14%	58.13%	65.64%
Returnil System Safe		70.74%	62.23%	66.40%	66.45%	66.76%	66.53%
Rising Internet Security		47.04%	42.85%	37.65%	42.51%	39.40%	41.73%
Security Coverage SecureIT 2011		95.34%	93.02%	94.71%	94.36%	86.76%	92.46%
Sophos Endpoint Security and Control		86.72%	85.60%	83.31%	85.21%	75.44%	82.77%
SPAMfighter VIRUSfighter		79.20%	63.21%	64.37%	68.93%	62.48%	67.32%
Total Defense Inc. Internet Security Suite Plus		80.56%	70.99%	64.10%	71.88%	59.30%	68.74%
Total Defense Inc. Total Defense r12		77.34%	67.15%	60.62%	68.37%	56.87%	65.49%
TrustPort Antivirus 2012		99.82%	99.71%	99.30%	99.61%	88.14%	96.74%
VirusBuster Professional		86.19%	81.47%	74.92%	80.86%	67.92%	77.62%

## OCTOBER 2011: WINDOWS SERVER 2003


















The platform for this test is the traditional *Windows Server 2003* which has been with us for quite some time. Having visited the platform most years since its release, preparation for the test was fairly straightforward.

The product deadline was set for 24 August, and the test sets were built around this date. The RAP sets were compiled using samples first seen in the three weeks before and one week following the deadline, and the trojans set and the worms and bots set were both put together from items gathered in the month prior to that period.

The WildList set was the first area to be affected by the recent changes to the way in which the list is compiled: the legacy naming scheme has been put into retirement, replacing the names that aim to reflect those used by

anti-malware solutions with less human-readable reference IDs for each sample. This meant some tweaks to the way the samples are processed, and all samples were re-validated regardless of whether they were new appearances on the list or long-time regulars.

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

Reactive And Proactive (RAP) scores October 2011	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost		81.89%	81.11%	72.74%	78.58%	67.14%	75.72%
AhnLab V3Net		83.12%	80.36%	74.34%	79.27%	69.83%	76.91%
ArcaBit ArcaVir*		NA	NA	NA	NA	NA	NA
Avast! Free Antivirus		96.27%	94.31%	89.21%	93.26%	79.69%	89.87%
Avertive VirusTect		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
AVG Internet Security		95.79%	93.52%	85.93%	91.75%	74.39%	87.41%
Avira AntiVir Server		98.65%	97.69%	92.49%	96.27%	86.38%	93.80%
BitDefender Security for File Servers		97.79%	97.69%	95.73%	97.07%	87.75%	94.74%
BullGuard Antivirus 10		97.72%	97.44%	95.31%	96.82%	87.29%	94.44%
Central Command Vexira		80.17%	79.18%	70.60%	76.65%	64.82%	73.69%
Clearsight Antivirus		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
CommTouch Command		67.81%	68.85%	66.73%	67.80%	66.41%	67.45%
Comodo Antivirus		88.31%	82.23%	76.72%	82.42%	69.99%	79.31%
Comodo Internet Security		88.31%	82.23%	76.72%	82.42%	69.99%	79.31%
Coranti Cora Antivirus		64.81%	67.61%	67.74%	66.72%	66.32%	66.62%
Defenx Security Suite 2012		82.24%	81.45%	73.33%	79.00%	67.59%	76.15%
Digital Defender		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
eEye Blink Server		81.23%	77.43%	75.36%	78.01%	73.12%	76.79%
Emsisoft Anti-Malware		98.78%	98.38%	96.73%	97.96%	86.69%	95.14%
eScan Internet Security		97.75%	97.40%	94.00%	96.38%	86.32%	93.87%
ESET NOD32 Antivirus		94.40%	92.04%	91.35%	92.60%	84.50%	90.57%
ESTsoft ALYac		96.83%	96.20%	92.47%	95.17%	84.95%	92.61%

### ESET NOD32 Antivirus 4

Version 4.2.71.2, Virus signature database 6406

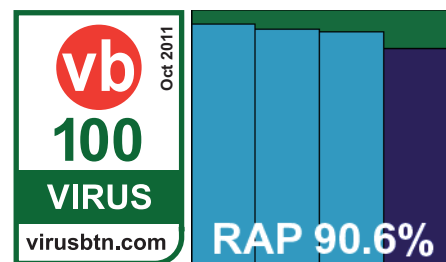
<b>ItW</b>	100.00%	<b>Worms &amp; bots</b>	96.78%
<b>ItW (o/a)</b>	100.00%	<b>Polymorphic</b>	100.00%
<b>Extd. WL</b>	100.00%	<b>Trojans</b>	96.75%
<b>Extd. WL (o/a)</b>	100.00%	<b>False positives</b>	0

















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

Speed measures showed decent scan times and reasonable overheads on access, with fairly low use of resources and

fairly low impact on our suite of tasks. Detection rates were superb, with very solid coverage of all the sets, the reactive parts of the

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



Reactive And Proactive (RAP) scores October 2011 Contd.	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Fortinet FortiClient		93.58%	92.79%	90.67%	92.35%	80.39%	89.36%
Frisk F-PROT		64.90%	67.69%	66.52%	66.37%	66.39%	66.38%
F-Secure Anti-Virus**		97.24%	97.36%	94.27%	96.29%	86.92%	93.95%
G Data AntiVirus		99.72%	99.64%	97.32%	98.89%	88.92%	96.40%
GFI VIPRE Antivirus		97.94%	98.03%	90.32%	95.43%	78.37%	91.17%
Hauri ViRobot Server		95.85%	95.10%	93.54%	94.83%	85.75%	92.56%
Iolo System Shield		63.90%	64.71%	62.22%	63.61%	62.27%	63.28%
Kaspersky Endpoint Security 8		93.04%	88.88%	89.49%	90.47%	82.27%	88.42%
Lightspeed Total Traffic Control		36.00%	33.89%	33.66%	34.52%	36.37%	34.98%
Lumension EMSS**		82.10%	81.34%	79.68%	81.04%	73.25%	79.09%
Microsoft Forefront		88.35%	84.17%	80.12%	84.21%	72.92%	81.39%
Norman Endpoint Protection		82.31%	78.33%	76.38%	79.01%	74.02%	77.76%
Preventon Antivirus Server		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
Quick Heal		78.78%	56.79%	61.56%	65.71%	73.57%	67.68%
Returnil System Safe		68.66%	69.67%	67.57%	68.63%	67.08%	68.25%
Rising Internet Security*		NA	NA	NA	NA	NA	NA
Sophos Endpoint Security and Control		83.76%	82.57%	79.34%	81.89%	71.56%	79.31%
SPAMfighter VIRUSfighter PRO		78.84%	75.74%	65.48%	73.35%	63.42%	70.87%
TGSoft VirIT eXplorer		30.17%	29.62%	32.07%	30.62%	31.35%	30.80%
Total Defense Inc Total Defense r12		70.77%	65.44%	59.82%	65.34%	56.64%	63.17%
UtilTool Server Antivirus		80.42%	77.15%	67.66%	75.07%	65.76%	72.75%
VirusBuster for Windows Servers		80.17%	79.18%	70.60%	76.65%	64.82%	73.69%

\* Testing not possible

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

## DECEMBER 2011: WINDOWS 7 PROFESSIONAL

This month saw some major changes and a radical overhaul of our test methodology. While some parts remain much as before, a swathe of tweaks and adjustments have accompanied a significant shift of focus, which now sees most of our tests – including the core certification components – running with live Internet access, allowing for improved detection from ‘cloud’ look-up systems (and which, of course, also increases the chances of false positives). The changes should make our performance measures more accurate, taking into account the time taken to perform look-ups and the added effort of polling for updates. The core certification set has also been expanded to include the new Extended WildList set, which covers a wider range of malware types. Full details of the new methodology

can be found at <http://www.virusbtn.com/vb100/about/methodology.xml>.

### ESET NOD32 Antivirus 5




















Main version: 5.0.94.0

**ItW Std** 100.00% **ItW Std (o/a)** 100.00%

**ItW Extd** 100.00% **ItW Extd (o/a)** 100.00%

**False positives** 0

















Looking to continue an epic run of success into our new testing format, *ESET*'s product came as a petite 52MB package including all required updates. Set-up was straightforward and fairly quick, and online updates were fast and easy too, with most installs completing in under five minutes.

Reactive And Proactive (RAP) scores December 2011	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
Agnitum Outpost*		70.14%	70.40%	60.05%	66.86%	70.67%	67.82%
AhnLab V3		73.18%	69.86%	68.12%	70.38%	76.92%	72.02%
Auslogics Antivirus		98.90%	98.56%	97.21%	98.22%	91.67%	96.59%
avast! Free Antivirus		98.01%	96.40%	92.16%	95.52%	84.46%	92.76%
AVG Internet Security		96.43%	92.65%	93.57%	94.22%	81.35%	91.00%
Avira AntiVir Free		99.07%	97.37%	96.52%	97.65%	90.25%	95.80%
Avira AntiVir Pro		98.84%	97.18%	96.27%	97.43%	90.02%	95.58%
BitDefender Antivirus Plus		99.20%	98.75%	97.40%	98.45%	91.74%	96.77%
BullGuard Antivirus 10		99.08%	98.64%	97.21%	98.31%	91.31%	96.56%
Central Command Vexira		N/T	N/T	N/T	N/T	N/T	N/T
Clearsight Antivirus *		64.19%	53.87%	53.28%	57.11%	66.32%	59.41%
CommTouch Command		62.21%	57.33%	60.65%	60.06%	69.99%	62.55%
Comodo Antivirus		79.56%	68.51%	64.96%	71.01%	63.97%	69.25%
Comodo Internet Security		79.56%	68.50%	64.95%	71.00%	63.97%	69.24%
Coranti 2012		99.30%	99.08%	98.55%	98.98%	93.04%	97.49%
Coranti Cora Antivirus		99.36%	99.12%	98.59%	99.02%	93.09%	97.54%
Defenx Security Suite 2012*		66.15%	57.18%	62.32%	61.88%	68.17%	63.46%
Digital Defender*		60.29%	59.77%	55.41%	58.49%	65.09%	60.14%
eEye Blink Professional		85.53%	79.48%	75.00%	80.00%	80.26%	80.07%
Emsisoft Anti-Malware		98.37%	97.94%	99.66%	98.66%	98.17%	98.53%
eScan Internet Security		99.07%	98.63%	96.99%	98.23%	91.27%	96.49%
ESET NOD32 Antivirus		96.99%	95.38%	93.56%	95.31%	86.45%	93.09%
ESTsoft ALYac		98.76%	97.86%	93.38%	96.67%	87.42%	94.36%
Filseclab Twister		88.21%	80.13%	78.87%	82.40%	72.02%	79.81%
Fortinet FortiClient		91.92%	89.19%	94.48%	91.87%	85.70%	90.33%
Frisk F-PROT		56.04%	48.90%	52.65%	52.53%	68.29%	56.47%
F-Secure Client Security		99.04%	98.52%	95.85%	97.80%	90.42%	95.96%

Key:

N/T – Not testable

\* Problems gathering data

Reactive And Proactive (RAP) scores December 2011 contd.	VB100	Reactive			Reactive average	Proactive Week +1	Overall average
		Week -3	Week -2	Week -1			
G Data AntiVirus 2012		99.89%	99.65%	97.24%	98.93%	92.12%	97.23%
GFI VIPRE Antivirus		98.32%	97.96%	94.08%	96.78%	81.37%	92.93%
Ikarus virus.utilities		98.15%	96.82%	95.30%	96.76%	88.29%	94.64%
Iolo System Shield		53.23%	46.51%	50.20%	49.98%	65.29%	53.81%
K7 Total Security		86.17%	82.96%	82.61%	83.91%	71.31%	80.76%
Kaspersky Endpoint Security 8		96.36%	93.56%	96.23%	95.38%	86.94%	93.27%
Kaspersky Internet Security 2012		95.67%	93.38%	96.06%	95.04%	86.77%	92.97%
Lavasoft Ad-Aware Total Security		99.88%	99.73%	97.29%	98.97%	91.99%	97.22%
McAfee VirusScan Enterprise		84.80%	77.36%	69.75%	77.30%	78.25%	77.54%
Microsoft Security Essentials		92.05%	88.47%	75.66%	85.39%	78.07%	83.56%
Nifty Security 24		95.04%	92.51%	94.05%	93.87%	85.06%	91.67%
Norman Security Suite		84.46%	75.69%	68.15%	76.10%	79.16%	76.86%
PC Tools Internet Security		79.39%	81.11%	86.94%	82.48%	81.85%	82.32%
PC Tools Spyware Doctor		79.45%	81.18%	87.00%	82.54%	81.90%	82.38%
Preventon Antivirus*		59.43%	55.14%	51.82%	55.46%	64.97%	57.84%
Qihoo 360 SD		97.01%	96.13%	92.24%	95.13%	86.26%	92.91%
Quick Heal Total Security 2012		78.58%	74.83%	64.26%	72.56%	75.22%	73.22%
Returnil System Safe 2011		63.26%	58.17%	61.01%	60.81%	70.22%	63.16%
Sophos Endpoint Security and Control*		86.75%	84.57%	83.50%	84.94%	76.41%	82.81%
SPAMfighter VIRUSfighter PRO*		70.92%	59.07%	54.24%	61.41%	67.22%	62.86%
Symantec Norton Internet Security		N/A	N/A	N/A	N/A	N/A	N/A
Total Defense Inc ISS Plus		70.55%	64.66%	60.29%	65.17%	63.29%	64.70%
Total Defense Inc Total Defense r12		69.59%	63.74%	59.70%	64.34%	61.61%	63.66%
TrustPort Antivirus 2012		99.56%	99.45%	95.73%	98.25%	91.14%	96.47%
UtilTool Antivirus*		59.40%	62.87%	49.70%	57.32%	31.65%	50.91%
VirusBuster Professional		N/T	N/T	N/T	N/T	N/T	N/T
Webroot SecureAnywhere		N/A	N/A	N/A	N/A	N/A	N/A

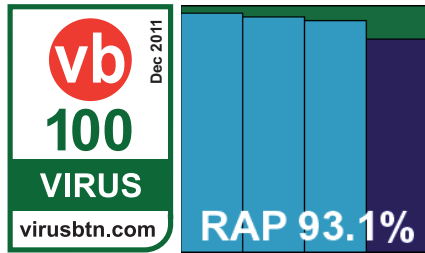
Key:

N/A – Not applicable

N/T – Not testable

\* Problems gathering data

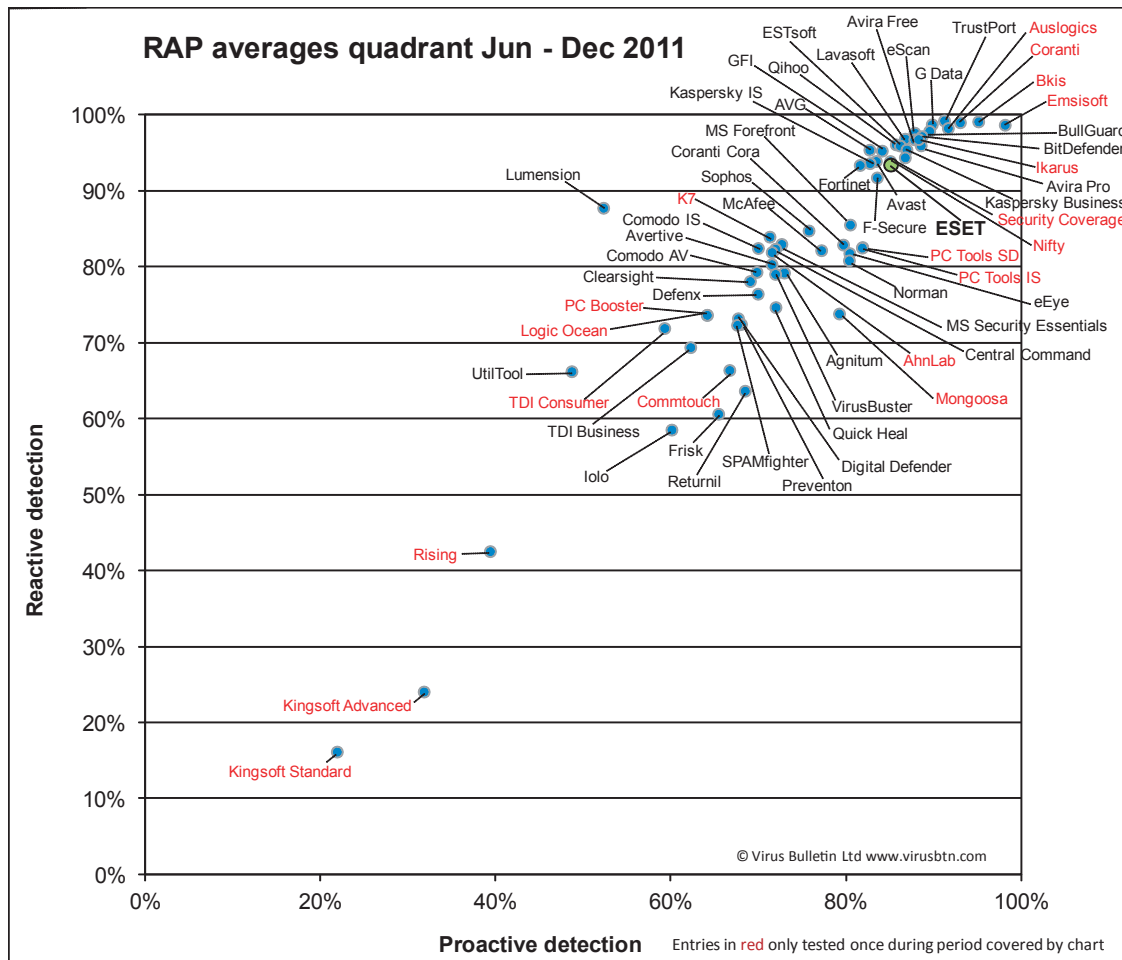
The GUI is very slick and attractive – a little more angular than expected, but still pleasant to look at and easy to use, with some improvements to the layout making the in-depth configuration easier to work with. Testing ran through simply, with good initial speeds and much faster speeds in the warm runs. Light overheads were recorded, with slightly higher than average RAM use but reasonable use of CPU cycles and average impact on our set of tasks. Detection rates were solid, dropping off slightly in the proactive week of the RAP sets but maintaining a good level throughout the Response tests. The core sets were handled



impeccably, comfortably earning *ESET* another VB100 award and continuing the vendor’s unbroken run of passes. *ESET*’s record cannot be faulted, with 12 passes in the last two years. Testing this month was interrupted by a single interface crash under heavy pressure, but protection was not affected and simply reopening the GUI proved sufficient to get things moving along again. All tests completed in well under the allotted two days.



*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/.*



The cumulative RAP quadrant gives a quick visual reference as to products’ reactive and proactive detection rates over the last four tests.