



TECHNOLOGY INSIGHTS

Internet Security 2010

Making Sense of Confounding Tests

For years now, we've relied on AV-Comparatives to provide reliable guidance on anti-malware products. The lab has a tradition of naming winners at the end of the year, and it has just done so for 2009. The top gong went to Symantec, which does not sit well with those of us who grew up with Norton and watched it put on so much flab that it weighed heavily on any PC, regardless of hardware specs.

The crushing weight was one turn-off; another was a set of manners that reminded us of school bullies: 'You'll wait until I'm finished, you will reboot now, you will get your turn when I'm good and ready.' That kind of stuff. For an entertaining read of what life was like with Norton back then, check:

In the Grip of Security – a user's vain attempts to reason with the antivirus mafia
http://www.technoledge.com.au/pdfs/grip_of_security.pdf

Back to the future

At Technoledge we ended up using ESET, once we ditched Norton and dived with a few others, in part because ESET NOD32 was AV-Comparative's winner in 2007. In 2008, NOD32 was a close runner-up to Avira, another great but little-known security product. This year, Avira dropped out of the top 3, mostly because it gave too many false positives.

AV-Comparative's annual ratings are a compound of results in various tests conducted over the year. The more Advanced+ ratings the software gets, the higher it ranks.

	On-Demand Test February 2009	Retrospective Test February 2009	On-Demand Test August 2009	Retrospective Test August 2009	Removal Test September 2009	PUP Test November 2009	Dynamic Test December 2009	Performance Test December 2009
avast!	ADV	STD	ADV+	ADV+	ADV	ADV	ADV	ADV+
AVG	STD	STD	ADV	ADV	ADV	ADV	STD	ADV
AVIRA	ADV	ADV	ADV	ADV	ADV	ADV+	ADV	ADV+
BitDefender	ADV	ADV	ADV+	ADV+	ADV+	ADV+	ADV	ADV
oScan	ADV	ADV	ADV+	ADV+	ADV+	ADV+	STD	STD
ESET NOD32	ADV+	ADV+	ADV+	ADV+	ADV	ADV	ADV	ADV+
F-Secure	ADV	STD	ADV+	ADV+	ADV+	ADV+	ADV	ADV+
G DATA	ADV	ADV	ADV+	ADV+	STD	ADV+	ADV	ADV
Kaspersky	ADV+	ADV+	ADV	ADV+	ADV+	ADV	ADV+	ADV+
Kingsoft				STD		STD		ADV+
McAfee	ADV+	ADV	ADV	STD	ADV	ADV+	STD	ADV+
Microsoft	STD	ADV+	STD	ADV+	ADV+	ADV	ADV	ADV+
Narman				STD	STD	STD		ADV
Sophos	STD	ADV		STD	ADV	ADV	N/A	ADV+
Symantec	ADV+	ADV	ADV+	ADV	ADV+	ADV+	ADV+	ADV+
TrustPort	ADV	STD	ADV	STD	ADV	ADV+	STD	STD

These are our own opinions.

We have no commercial arrangements with vendors.

For more reviews, please contact [TECHNOLEDGE](mailto:info@technoledge.com.au).

T +61 2 9909 0246
E info@technoledge.com.au
W www.technoledge.com.au

Using that system, Norton comes out on top, followed by Kaspersky and ESET, with Bitdefender and F-Secure hot on their heels. The lab makes the point that all the

products it tests are decent, since really poor performers – big names like Trend Micro and CA among them – aren't even included. For the full report, click on 'Summary Report 2009' in the top right-hand corner at <http://www.av-comparatives.org/> .

Real world testing

The last couple of years have seen a number of security analysts chastise the AV-software industry for arranging tests that only fools wouldn't pass since even the so-called 'in-the-wild' list of malware was published to each participating company before testing. All they had to do was to ensure that they had every gremlin's signature in their databases.

Pressure mounted on test labs to introduce real-world testing that would pitch security suites against a more realistic mix of malware, and also evaluate its user interface and effect on PC performance. [AV-Test.org](http://www.av-test.org) was the first major lab to attempt such a test. (Results courtesy of <http://www.pcmag.com/article2/0,2817,2357347,00.asp>)

MALWARE DETECTION RATES AND WARNING MESSAGES (FALSE ALARMS)

Tested Product	Malware Detected	False Alarms
Symantec Norton Internet Security 2010	98.0%	almost none
Kaspersky Internet Security 2010	97.5%	few
PC Tools Internet Security 2010	95.8%	almost none
AVG Internet Security 9.0	92.2%	few
G Data Internet Security 2010	90.0%	many
Panda Internet Security 2010	90.0%	almost none
Avira Premium Security Suite 9.0	87.7%	many
McAfee Internet Security 2010	87.2%	few
CA Internet Security 2010	86.7%	few
F-Secure Internet Security 2010	85.8%	almost none
BitDefender Internet Security 2010	84.3%	few
Trend Micro Internet Security 2010	83.3%	few

MALWARE BLOCKING RATES AND WARNING MESSAGES (FALSE ALARMS)

Tested Product	Malware Blocked	False Alarms
PC Tools Internet Security 2010	94.8%	none
Symantec Norton Internet Security 2010	92.8%	none
Kaspersky Internet Security 2010	89.8%	few
Panda Internet Security 2010	88.7%	none
Avira Premium Security Suite 9.0	87.2%	none
McAfee Internet Security 2010	86.7%	none
AVG Internet Security 9.0	84.2%	few
G Data Internet Security 2010	83.0%	few
Trend Micro Internet Security 2010	81.3%	few
F-Secure Internet Security 2010	80.2%	none
BitDefender Internet Security 2010	77.8%	none
CA Internet Security 2010	73.5%	none

The lab analysed each product's ability to detect threats and block their installation, regardless of the protection mechanisms employed. This is a better idea than testing the on-demand scanner alone, or a product's heuristic detection ability.

This kind of dynamic testing should be more representative of real life, and AV-comparatives followed suite late last year with what they called a 'Whole Product Dynamic Test' (the link is on their website in the same corner as the 2009 summary report - they'd rather we didn't use direct links). Symantec, Kaspersky and Avira are the top 3 here, with 97 to 99 out of 100 threats blocked. The next bunch is made up of Microsoft Security Essentials (!?), Avast, Gdata, F-Secure, ESET and Bitdefender. McAfee is the big loser here, managing just 86 blocked threats.

Real world questions

Apart from the top two, AV-Test.Org's results aren't anything like AV-comparatives'. McAfee rates poorly but is still ahead of Bitdefender and F-Secure, solid top-six performers everywhere else. And for Trend Micro to be ahead of them is a big surprise (TM has rarely performed well in these tests), but now we have an ad from TM proclaiming that it's come first in a different 'real-world' test <http://apac.trendmicro.com/apac/competitive-benchmarks/>

The lab that produced these results is NSS, a brand new lab that uses a 'Live-in-the Cloud' test framework to focus on testing how well Internet Security suites protect from web-based threats. If the previous two sets of results are confounding, those from NSS Labs make the mind boggle:

Product	Caught Initially on Download	Caught Subsequently on Execution	Total
Trend Micro	91.0%	5.5%	96.4%
Kaspersky	78.5%	9.3%	87.8%
Norton	50.5%	31.3%	81.8%
McAfee	79.8%	1.9%	81.6%
Norman	66.3%	14.9%	81.2%
F-Secure	63.7%	16.4%	80.0%
AVG	65.0%	8.3%	73.3%
Panda	64.4%	7.6%	72.0%
ESET	65.4%	2.5%	67.9%

The only thing that is sillier than for Trend Micro to come first is for ESET to come last. These results make no sense in any known context, so we'll ignore them.

Can elephants really learn to dance?

Symantec has claimed for some time now that it listened to its users (how many years did it take?) and redesigned Norton IS to float like a butterfly, but most of us didn't believe it. That Symantec (with McAfee) was fined millions last year for 'auto-renewing' annual licences without their users' approval didn't endear the company to us either. That clause was buried deep in the EULA, which most people simply don't read because they expect big brand companies to be up-front about these things.

Neil Rubenking at PC Magazine has been testing AVs since he was a callow youth. His long support of Norton has troubled us, but Neil's reputation as the eminence grise of AV-testers cannot be ignored. Here's his take on current Internet Security suites <http://www.pcmag.com/article2/0,2817,2351871,00.asp> .

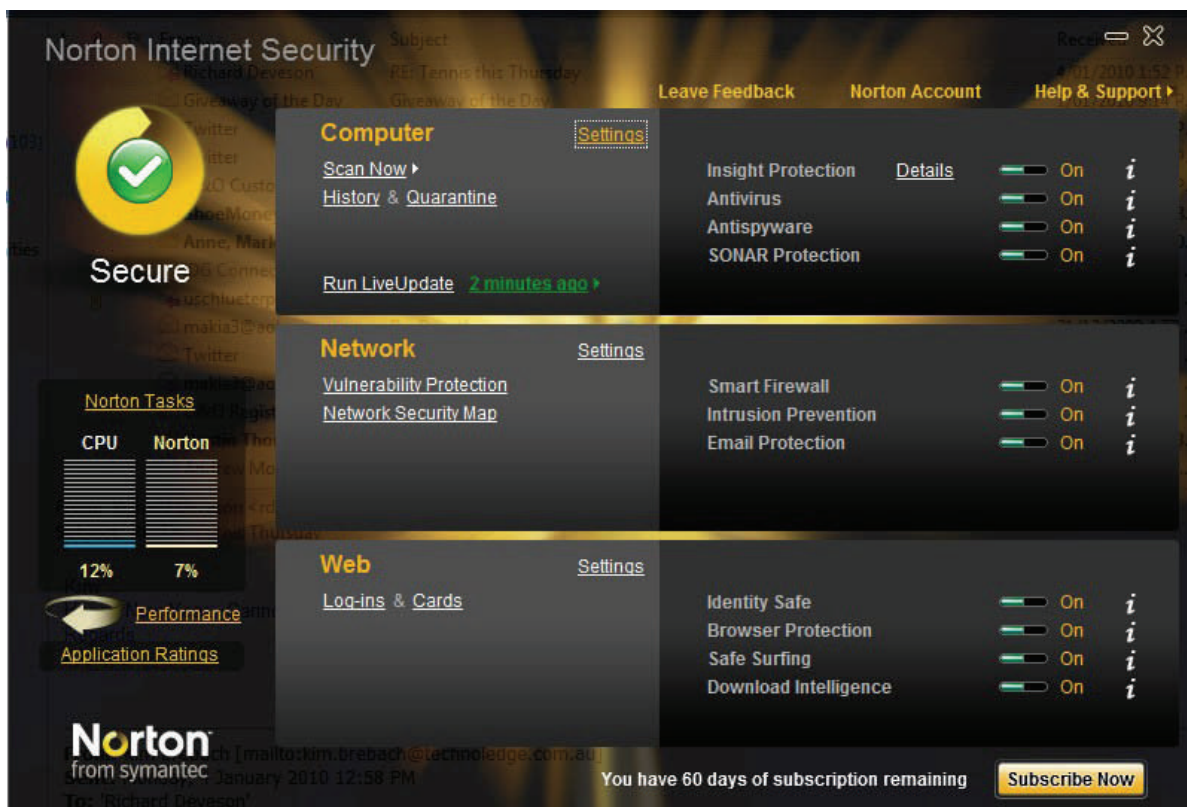
With AV-Test.Org and AV-Comparatives and Neil Rubenking all singing the praises of Norton Internet Security 2010, and waxing lyrical about its light hand and velvet footprint, we began to wonder whether Norton could really change so much.

There's one way to find out

The Norton IS 2010 trial on offer at the company's website is an **opt-out** trial. What's an opt-out trial? You have to opt out before the 30 days are up or they'll charge your credit card. More of the same. I find a trial on the PC Authority website for 60 days and download the software. Symantec bugs me as soon as it's installed and I've activated the account. Yes, it bugs me to buy NIS 2010 3 seconds into the trial. Great marketing, Symantec.

The rest of it? It's a different product from the one I likened to the Mafia - it seems that elephants can be taught to dance after all. The problems is that leopards can't change their spots. The first giveaway is the 100mb download, but the install is fast and free from all those reboots and updates that used to make us froth at the mouth. There are 25mb of updates to come but their installation is fast as well. The Quickscan it offers takes just minutes and finds 66 tracking cookies.

NIS takes a backseat while I buzz around online, and the interface is much improved as well, with the 'Settings' option bringing up more detailed panels that let you tweak just about everything to your heart's content.



Boot times on my test Vista laptop are 10-20 seconds slower than with Bitdefender, our current bodyguard. Bitdefender had already added 30 seconds to ESET's boot time but took up only around 20mb of RAM once settled down. NIS 2010 shows two components, one taking between 5 and 130mb of RAM depending on whether its idle or doing something, and another taking between 5 and 45mb.

10 - 175mb of RAM is quite a range and suggests that Symantec's engineers have found away to hide that bulk and run lean unless it's busy. Then the heavies come out briefly but here's no drag when you work, the updates are fast, the spam filter is accurate right out of the box and doesn't make a mess of Windows Mail. We really can't find much wrong with it.

Would we buy it?

No. Yes, it's a vastly improved product, top-ranked by several reputable labs or testers. Frankly, we'd rather support smaller companies like Bitdefender, ESET or Avira, and we're pretty sure Symantec doesn't need our business - six copies of security software for our office.

Reality check: as we keep stressing, no single solution will keep you safe from all harm, you can see that from the lists above and the one below, and that 2% gap is enough to let in plenty of evil spirits - you'd be more than unwise to rely on one security solution. That's why we run and recommend a solid IS suite together with Intrusion Protection software like PREVX-3 or Threatfire.

One Last Word on Spyware

Neil Rubenking at PC Magazine produced this very interesting graph a few months back when he tested the ability of Internet Security suites to block and remove spyware.

PRODUCT	Suite	Malware Removal	Malware Blocking	Keylogger Removal	Keylogger Blocking
BitDefender Total Security 2010	Y	7.5	9.4	4.8	5.5
eScan Internet Security Suite 10	Y	7.0	8.8	4.1	4.4
Hitman Pro 3.5		6.6	n/a	5.6	n/a
k7 TotalSecurity Version 10.0	Y	6.8	9.3	5.9	7.4
Kaspersky Internet Security 2010	Y	6.7	8.6	1.6	3.0
Malwarebytes' Anti-Malware 1.36		6.5	n/a	0.5	n/a
Microsoft Security Essentials beta		7.0	7.9	1.8	2.3
Norton 360 version 3.0	Y	7.3	8.7	6.1	6.8
Norton Internet Security 2010 beta	Y	8.0	9.6	6.8	7.3
Panda Cloud Antivirus		6.5	8.3	3.8	6.0
Panda Internet Security 2010	Y	7.7	7.1	6.2	4.2
Prevx 3.0		7.0	9.4	6.0	8.9
Spyware Doctor with AntiVirus 6		6.7	8.3	4.8	9.0
ThreatFire 4.5		n/a	7.8	n/a	3.0
Webroot AntiVirus with AntiSpyware 6.1		6.8	8.3	6.8	8.5

A few curious points come out of this:

The dedicated spycatchers (Webroot, Spyware Doctor) don't block spyware as well as the best IS suites (NIS 2010 and Bitdefender 2010)

- These results are not at all consistent with those listed above for AV-Test.Org
- Kaspersky and Microsoft Security Essentials fare pretty badly with spyware here
- Malwarebytes Anti-Malware clearly gave Neil all kinds of problems
- Norton IS 2010 turns in better results than Norton 360. How can that be?
- The gaps for evil spirits to creep through are 4 - 6% even with the best products, so we repeat the previous advice: use two solutions of different types.

Products like PREVX3 or Threatfire may produce numerically similar results as suites like NIS 2010, but work in a very different way and will catch stuff the other misses and vice-versa. Add a website checker like WOT and you might get close to 100% protection, especially if you use common sense when working on line.

#