



TECHNOLOGY INSIGHTS

2008 Internet Security Suites Tested Are they getting the Message?

Part 1 - Is there Truth in Numbers?

Security expert Bruce Scheiner talks about the 'security theatre', where vendors make their customers feel secure 'by offering protection against threats that were not that great in the first place.' He adds that 'buyers can't tell the difference between good and bad [products]' and that many security vendors 'play on emotion and fear'.

That about sums up the state of affairs. The old mafia families Norton, McAfee and Trend Micro have sold millions of clunky products to fearful consumers. In recent years, cheeky newcomers have muscled in on the old mafia's turf, promising better protection and milder manners.

Symantec responded by claiming that a new version of Norton, the elephant in the PC security room, could dance like a ballerina, while McAfee and Trend Micro put on more weight and lumbered on. Zone Labs' newer security suite flattered the old guard by matching their bulk. Then Microsoft decided to get into the security race and promptly collapsed on the first lap, winning the wooden spoon in the VB 100 tests.

Microsoft changed the rules, though, adding PC maintenance and file backup to its list of features. Symantec and McAfee, faced with the biggest threat they'd ever detected, readied new products to take on Windows Live-One Care. Microsoft tightened the screws some more, claiming that Vista was so secure it needed no extra guards.

With their turf under threat from two sides, the old mafia families decided to make their offers harder to refuse. They threw in three security guards for the price of one and added other attractions like parental control and phishing protection.

No Surety in Security

Security was always too arcane for ordinary folks to get their heads around. Finding decent anti-malware programs is a lot like finding a good dentist: in both cases, you don't know how painful they can be until you're in the hot seat. And there's no easy way to establish the long term worth of the short term pain.

Independent test labs offer some insights for the diligent, but some of them simply certify products for a fee paid by vendors keen to put reassuring stickers on their boxes. Even the real tests are hardly representative of the real world, since the vendors all have a copy of the script, like actors rehearsing for a play.

PC magazines and tech websites run regular security reviews but few have any real capacity for testing AV-products. **PC Magazine** and **Australian PC User** do. **PCWorld** gets AV-Test.org to run tests for them. A few technology veterans do their own tests, among them Neil Rubenking, the eminence grise of security at PC Magazine, Robert Vamosi at CNET, Gizmo at Techsupportalert.com and Scot Finney at Scot's Newsletter.

Sadly, there's a whiff of suspicion that advertisers influence the results of

These are our own opinions.

We have no commercial arrangements with vendors.

For more reviews, please contact [TECHNOLEDGE](#).

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

certain publications, so I tend to rely on Gizmo and Scot more than the rest (since they're independent spirits). A few websites that review security products even have affiliate links with AV-vendors and get kick-backs out of every click on links to their products.

Most test labs only reveal their results for payment, but those of **Virus Bulletin** are often published by vendors who do well. **AV-Test.org**'s results are just as hard to come by, and **Check-Vir** only publishes overall ratings on its website. That leaves **AV-Comparatives** as the one independent lab that provides the full details on its website, <http://www.av-comparatives.org>

After some diligent digging, I've managed to come up with these product rankings:

	AV-Comp	PCWorld	Check-Vir	(AV-Test.org)
Antivir (paid)	Advanced +			2
AVG (paid)	Advanced +	recommended	Standard	6
Bitdefender	Advanced +	Top score		1
F-Secure	Advanced +			4
Kaspersky	Advanced +	Top score		3
NOD32	Advanced +	Top score	Advanced	
Norton	Advanced +	Top score	Standard	7
McAfee	Advanced		Advanced	
Trend Micro	Standard	recommended	Standard	
CA (e-Trust)	Below Standard		Standard	5
Avast (paid)	Advanced	recommended		
Panda	Not tested	recommended	Standard	
Bullguard	Not tested		Advanced	
Microsoft	Standard			8

Notes

AV-Comparatives uses a 3-tier rating system.

Most products are tested in 'comparatives' but **Trend Micro** and **CA** were tested on their own. TM scraped into a Standard rating but CA didn't make the grade.

Panda and **Bullguard** are not included in tests.

Newcomers like **Comodo** and **Clam-Win**, tested in a separate group, posted results that were even less impressive.

- PCWorld** uses AV-Test.org but presumably also evaluates other aspects of security suites There's just one point separating the top 4 here, then a big gap to the rest, that's why I split them into 'top score' and 'recommended'. <http://www.pcworld.com/article/id,130869/article.html>
- Check-Vir** uses a simple 2-tier rating system and doesn't publish details.
- AV-Test.org** lists products in order of performance, lower being better here.
- I've excuded **Trustport**, **Fortinet** and **Webwasher** (all top-rated by several labs) from this review since they are aimed more at the business market.
- Gdata's AVK** (AntiVirusKit) also rates highly but was difficult to find English language reviews on (more below).

Looking for Consistent Results

The **AV-Test.org** results stand in stark contrast to the **PCWorld** rankings posted a few months earlier this year (2007). It was hard to believe that **Microsoft** came in ahead of **NOD32, McAfee, Trend Micro** and **Sophos**, even for Andreas Marx who heads up AV-Test.org. The best he could do was to suggest 'that the high amount of malware researchers Microsoft has hired from other AV companies (including many people from Symantec, McAfee, Trend Micro, F-Secure and CA) has paid off.'

<http://news.softpedia.com/news/Microsoft-039-s-Security-Solutions-Explode-Top-Sophos-Nod32-McAfee-and-Trend-Micro-63834.shtml>

'We are not convinced!' as German foreign Minister Joshka Fischer said to Donald Rumsfeld when he was rounding up allies for the invasion of Iraq. After all, Microsoft's offering has bombed out in other tests, like those run by Virus Bulletin.

AV-Comparatives publishes all the gory details of its extensive tests but asks that other sites link only to their main page, <http://www.av-comparatives.org/>, that's the reason I've not provided direct links to specific pages in this article. Clicking on 'comparatives' (on the left) takes visitors to a listing of all available test reports.

It's encouraging to find that the top 4 in the PCWorld test all score an Advanced+ rating with AV-comparatives, and few would argue with a top list that includes **Bitdefender, Kaspersky, NOD32** and **Norton**.

AV-Test.org has **AntiVir** and **F-Secure** in the top 4, along with **Bitdefender** and **Kaspersky**. Gizmo rates Antivir among the top products (**NOD32** and **Kaspersky** being the other two), and Scot Finney chose **F-Secure** as his AV of 2006 until it proved too intolerant of other security products. Scot's choice for 2007 is **NOD32**, which tends to cause no conflicts with other programs.

A Different Ballgame

In 'on demand' tests, AV-Comparatives feeds thousands of bad bugs to various malware engines. AV-C also runs proactive/ retrospective tests, which are more revealing. This test uses versions of products that have not been updated for 3 months to see how good their heuristics are at catching malware that has surfaced since the last updates. Highest is best here.

Antivir	71%	Standard	(penalized for high rate of false positives)
NOD32	68%	Adanced+	
Bitdefender	48%	Standard	(penalized for high rate of false positives)
Kaspersky	35%	Standard	
F-Secure	31%	Advanced	
AVAST	26%	Advanced	
Norton	24%	Advanced	
McAfee	24%	Advanced	
Microsoft	18%	Standard	
AVG	8%	No rating	(poor detection and high false positives)

Top Guns

We now have a fair degree of consensus on the top 4 and, taking other scores into account, we should probably add Norton and F-Secure to make up the top 6:

AntiVir
Bitdefender
F-Secure
Kaspersky
NOD32
Norton

The inclusion of **Norton** will raise hairs on the necks of many users, while the exclusion of **McAfee** will raise some eyebrows. To see if the old families have really changed their ways, as some reviewers claim, we take a look at them in the last section (3).

Trend Micro has won a place among the big three, but its poor record in independent tests makes it hard to take seriously for anything but its marketing muscle.

Zone Alarm Internet Security is a recent addition in its current form (with Kaspersky's AV and MailFrontier Spam Filter) and doesn't (yet) tend to feature in independent tests. That hasn't stopped it winning some big fans, among them Brian Livingstone of Windows Secrets and Robert Vamosi at CNET who gives it 8/10. 175 CNET readers give it 4.9/10. This kind of discrepancy between editorial ratings and real-world experience is common.

A few months back, I found ZAISS 7 a big drag – a 3 minute boot time on XP is Theatre of the Absurd. I checked on ZAISS 7.1 Vista reviews and it seems that making ZAISS work on Vista required brutal surgery by its makers.

According to Davey Winder at **PC Pro**, 'the casualties include IM security, privacy controls, ID lock, spy site blocking, ad blocking, cache cleaning, mobile code control, MailSafe protection and parental controls.' Despite the extensive liposuction, Winder complained that 'the performance of our Vista test PC ... went through the floor. Most obvious was the increase in boot time for Vista itself, up from a couple of minutes to ten minutes. Compared with Norton 360, the resource usage was also poor and apps took longer to start up.'

That made it easy to cross ZAISS off my list. I also tried hard to get some intelligence on **GData's (AVK) Internet Security 2008**, to help me decide if it was worth checking out. The German PC mag **Computer Bild** rated it tops but its summary gave a clue to the suite's dark side: 'Höchste Sicherheit mit hohem Ressourcen hunger,' translating to 'high security with a vast appetite for resources.'

The complaints from users on German forums confirm that this is the battleship Bismarck of security suites. The download is a staggering 310MB, bigger than some Linux distros I've tested. What do you get with it? 6 kilos of Bratwurst and a Litre of Bier?

New tricks

Gdata's suite is one of several who try to improve their detection rates by employing twin scanning engines (Kaspersky and Bitdefender in this case). F-Secure and Trustport also use more than one engine. This trend has a predictable impact on performance, but most security products are designed more with an eye on VB100 awards than on real world threats – that's where the theatre comes in.

Gizmo and others have shown that combining **different** layers of security tends to produce better results overall, and this even holds true when the individual layers are free products like AVG and Threatfire, a HIPS (Host Intrusion Protection System). Their combined footprint is much smaller than that of the twin-engine machines.

[PART 2 - Internet Security Suites](#)