

AV-Test release latest results

Major test of suite products completed

Independent testing body AV-Test.org has released the results of a major comparative of suite products, with many vendors' 2009 editions included in the results. The test covers a range of metrics, including detection rates over various types of malware including adware and spyware, false positive rates, scanning speed, proactive detection, and response times to outbreaks.

In terms of pure detection rates in on-demand scanning, a beta version of *GDATA's AVK 2009* topped the charts for both 'malware' (measured against 1,164,662 samples) and 'ad- and spyware' (94,291 samples), with *Avira's Premium Security Suite 2008* a close runner-up in the former category and *F-Secure 2009* placing second in the latter. *Secure Computing's Webwasher* gateway product, based on the *Avira* engine with some in-house heuristics, came third in both categories.

Other areas analysed were scored on a five-point scale from very good to very poor. 'Proactive' protection included scanning of files discovered after the freezing of products, and executing unrecognised malware to test behavioural protection. Products rating 'good' or better in every category include *Avira's* premium suite (the popular free version has less complete spyware detection), *AVK 2009*, *F-Secure's* 2009 suite, *Symantec's Norton I.S. 2009* (still in beta) and *Sophos's Security Suite 2.5*. All products taking part in the test managed to achieve a 'good' or better in at least one category.

The test also included keeping a record of the number of updates released over a four-week period. Of course, these numbers on their own cannot be used to measure the quality of the products involved, but were recorded out of interest. The most interesting data to emerge from this measurement was that the 2009 version of *Norton* topped the table with an impressive 6,202 incremental micro-updates, issued several times per hour, while *Kaspersky* came a distant second with a mere 696. Half of the 34 products tested had fewer than 100, including those from *McAfee* (21) and *Trend Micro* (30).

A summary of the major areas tested is printed below; hover over the product names to see full version information.

Product	malware on demand	adware / spyware on demand	false positives	scan speed	proactive detection	response times	malware on demand	adware / spyware on demand
AVK 2009 (G Data) (2)	++	++	+	+	++	++	99.8%	99.8%
AntiVir (Avira)	++	++ (4)	+	++	+	++	99.8%	99.0%
WebWasher-GW (3)	++	++	o	++	++	++	99.7%	99.2%
TrustPort	++	++	-	--	++	++	99.5%	98.4%
Avast! (Alwil)	++	++	+	+	o	o	99.3%	98.3%
Ikarus	++	++	o	+	+	+	99.5%	98.6%
F-Secure 2009	++	++	+	+	++	++	99.2%	99.6%
AVK 2008 (G Data) (1)	++	++	o	-	+	++	99.2%	99.1%
Norton 2009 (Symantec)	++	+	++	++	+	++	98.7%	95.4%
Kaspersky	++	++	o	o	+	++	98.4%	98.3%
F-Secure 2008	++	++	+	o	++	+	98.2%	98.4%
ZoneAlarm	+	+	o	o	+	++	97.8%	97.7%
eScan	+	+	o	-	+	++	97.8%	97.4%
Norton 2008 (Symantec)	+	o	++	+	+	o	97.8%	94.6%
Microsoft	+	+	++	o	-	-	97.7%	97.1%
BitDefender 2008	+	-	+	-	++	+	97.7%	87.8%
BitDefender 2009	+	-	+	o	++	+	97.6%	88.0%
Sophos	+	+	+	+	++	+	97.5%	95.0%
Norman	+	+	+	o	+	o	96.3%	95.8%
AVG	+	-(4)	+	+	o	o	95.8%	87.0%
F-Prot (Frisk)	o	o	+	+	o	o	94.8%	92.6%
Nod32 (Eset)	o	o	++	++	++	+	94.4%	94.7%
McAfee	o	o	++	o	+	-	93.6%	94.5%
Fortinet-GW	o	--	o	+	++	+	92.6%	81.9%
K7 Computing	o	o	o	++	-	o	92.1%	94.0%
Panda 2009	o	+	+	+	++	+	91.8%	95.6%
Trend Micro	o	-	+	+	o	+	91.3%	88.5%
VBA32	o	-	o	o	+	o	90.5%	85.2%
VirusBuster	-	-	+	+	o	o	89.0%	85.8%
ClamAV	-	o	-	--	-	++	88.5%	92.8%
Panda 2008	-	o	+	+	++	o	86.4%	93.4%
Dr Web	--	-	o	o	+	o	84.9%	89.6%
Rising	--	--	+	o	o	o	83.4%	77.5%
CA-AV (VET)	--	--	++	o	-	--	65.5%	68.0%
Index	malware on demand	adware / spyware on demand	false positives	scan speed	proactive detection	response times	malware on demand	adware / spyware on demand
++	>98%	>98%	no FP			< 2 h		
+	>95%	>95%	1-2 FP			2 - 4 h		
o	>90%	>90%	3-4 FP			4 - 6 h		
-	>85%	>85%	5-6 FP			6 - 8 h		
--	<85%	<85%	> 6 FP			> 8 h		

Notes

(1) AVK 2008 uses the Avast and Kaspersky scan engines

(2) AVK 2009 uses the Avast and BitDefender scan engines

(3) WebWasher uses the Avira engine and a self-developed heuristic engine

(4) the free (personal) edition does not include ad- and spyware detection, so the results would be --

