Anti-Virus Comparative

Summary Report 2008

Awards, winners, comments

Date: December 2008

Last revision: 9th December 2008

Website: http://www.av-comparatives.org

1. Introduction

At the end of every year, AV-Comparatives releases a summary report to comment on the various Anti-Virus products tested over the year, and to determine the winners in the various tests. Please bear in mind that this report includes all of the results achieved during the various tests of 2008, i.e. **not** only the latest ones. Comments and conclusions are based on the results contained in the various test reports of AV-Comparatives (www.av-comparatives.org/seiten/comparatives.html).

2. Overview of levels reached during 2008

Only high-quality Anti-Virus products with good detection rates can participate in the regular AV-Comparatives tests. It is important that readers understand that the STANDARD level/award is already a good score, since it requires the ability to detect a minimum percentage of malware. Many products that are not listed on AV-Comparatives would not reach the minimum requirements to participate; therefore the ones that are included in the tests of AV-Comparatives can be considered to be a selection of very good and high-quality Antivirus products.

Below the overview of levels/awards reached by the various Anti-Virus products in the main tests[1] of AV-Comparatives during 2008.

	February 2008	May 2008	August 2008	November 2008
	On-demand test	*Retrospective test*	On-demand test	*Retrospective test*
avast!	ADVANCED+	*STANDARD*	ADVANCED+	*STANDARD*
AVG	ADVANCED+	*ADVANCED*	ADVANCED+	*STANDARD*
AVIRA	ADVANCED+	*ADVANCED+*	ADVANCED+	*ADVANCED*
BitDefender	ADVANCED	*STANDARD*	ADVANCED	*STANDARD*
eScan	ADVANCED+		ADVANCED	
ESET NOD32	ADVANCED+	*ADVANCED+*	ADVANCED	*ADVANCED+*
F-Secure	ADVANCED+		ADVANCED	
GDATA AVK	ADVANCED+	*ADVANCED*	ADVANCED+	*ADVANCED*
Kaspersky	ADVANCED+	*STANDARD*	ADVANCED+	*ADVANCED*
McAfee	ADVANCED	*ADVANCED*	STANDARD	*ADVANCED*
Microsoft	ADVANCED	*ADVANCED*	STANDARD	*ADVANCED*
Norman	ADVANCED	*STANDARD*	ADVANCED	*STANDARD*
Sophos	ADVANCED		ADVANCED	
Symantec	ADVANCED+	*STANDARD*	ADVANCED+	*ADVANCED*
TrustPort	ADVANCED+		ADVANCED+	*STANDARD*
VBA32	STANDARD	*STANDARD*		*STANDARD*

Note: grey means certification level not reached

3. "Winners"

If you plan to buy an Anti-Virus, please visit the vendor's site and evaluate their software by downloading a trial version, as there are also many other additional features (e.g. firewall, behaviour blocker, spam-filter, etc.) and important considerations (e.g. compatibility, graphical user interface, ease of use, price, etc.) for an Anti-Virus that you should evaluate by yourself. As explained above, a perfect Anti-Virus or the best Anti-Virus for all needs and for every user does not exist. Our winners category is based purely on the objective test data and does not evaluate or consider other factors that may be of importance for specific users' needs or preferences.

[1] The following results are not included in the table because these were achieved in separate non-competitive tests of new technologies/products - Kaspersky had an ADVANCED rating in the May 2008 retrospective test and McAfee with Artemis technology had an ADVANCED+ rating in the on-demand test of August 2008.

a) Overall winner of 2008 based on the reached levels and results:
To be rated „Best Anti-Virus Product of 2008" by AV-Comparatives, an Anti-Virus product should have high detection rates, high proactive detection rates, very few false positives (zero is preferable), be fast with a low system impact, cause no crashes or hangs, and have no annoying bugs. The following products received at least 3 ADVANCED+ awards during 2008: AVIRA and ESET NOD32. It was very close, but the detailed scores of AVIRA were higher than the ones of ESET NOD32. The overall Best Anti-Virus product of 2008 is **AVIRA**

b) On-Demand detection winner:
The following products received the ADVANCED+ award in both overall on-demand detection tests of February and August 2008 (full-sets): Avast, AVG, AVIRA, GDATA, Kaspersky, Symantec. AVIRA and GDATA AVK achieved results over 99% in both tests, with AVIRA detecting a bunch of files more than GDATA AVK. Therefore, the On-Demand Detection winner is **AVIRA**

c) Proactive On-Demand detection winner:
The retrospective tests show how good the on-demand proactive detection of the various Anti-Virus products with highest settings is (how good they are at detecting on-demand new/unknown malware). A high (proactive) on-demand detection rate must be archived together with a low rate of false alarms. The following products received the ADVANCED+ award in both retrospective tests of May and November 2008: ESET NOD32. AVIRA had also very good scores (also with default settings) in both tests, but had a few more false alarms than ESET (which runs with highest settings by default). Therefore, the Proactive On-Demand Detection winner is **ESET NOD32**

d) False Positives winner:
False positives can cause as much troubles as a real infection. Due to this, it is important that Anti-Virus products have stringent Quality Assurance testing before release to public (in order to avoid false positives). The products with the lowest rate of false positives during 2008 were: McAfee (1) and Microsoft (6). Therefore, the product with the lowest rate of false alarms is **McAfee**

e) On-Demand Scanning Speed test winner:
The products with the highest on-demand throughput rate (green bars in both speed tests in May and August 2008) with best possible detection settings were AVIRA and Symantec, but Symantec was faster than AVIRA. So, the On-Demand Scanning Speed winner is **Symantec**

f) File copying / on-access scanning speed winner:
The following products added with default settings the lowest delay while copying/accessing files according to the performance test: Kaspersky (+28%) and ESET NOD32 (+31%). Therefore, the On-Access Scanning Speed winner is **Kaspersky**

g) Overall Performance test winner:
The following products got the ADVANCED+ rating in the Performance test (which aims to measure the impact of Anti-Virus software on system performance): ESET NOD32 (+22%), VBA32 (+22%), BitDefender (+22%), Symantec (+23%), GDATA AVK (+31%), AVIRA (+32%), Avast (+33%), McAfee (+37%), Microsoft (+40%). ESET NOD32 was one of the fastest products tested: esp. considering that like the McAfee and Microsoft products, it runs with the most secure configuration as default setting. Therefore, the overall Performance Test winner is **ESET NOD32**

Summary:

a) Overall / Best Anti-Virus of 2008: **AVIRA**
other candidates were: ESET NOD32

b) On-Demand detection: **AVIRA**
other candidates were: Avast, AVG, ESET NOD32, GDATA AVK, Kaspersky, Symantec, Trustport

c) Proactive on-demand detection rate: **ESET NOD32**
other candidates were: AVIRA

d) Lowest false alarm rate: **McAfee**
other candidates were: Microsoft

e) On-demand scanning speed: **Symantec**
other candidates were: AVIRA

f) File copying / On-access scanning speed: **Kaspersky**
other candidates were: ESET NOD32

g) Overall Performance: **ESET NOD32**
other candidates were: Avast, AVIRA, BitDefender, GDATA AVK, McAfee, Microsoft, Symantec, VBA32

4. Comments

Below some comments about the various products included in the test-series of 2008:

Avast (**www.avast.com**): In 2008 avast! improved once again and got for the first time two ADVANCED+ awards for its on-demand detection rates. The generic detections of Avast were also improved, but also the false alarm rates increased (probably due automated/fast additions of samples) and need to be better balanced.

AVG (**www.avg.com**): AVG Anti-Virus includes now in all products the Ewido engine in addition to the AVG engine. The detection rates of AVG improved further during 2008, earning two ADVANCED+ awards for its high on-demand detection rates. AVG includes also *Safe Surf*, which aims to protect against exploits and drive-by downloads while surfing.

AVIRA (**www.avira.com**): Also this year AVIRA showed very high detection rates, high proactive detection rates and a fast on-demand scanning speed. According to our tests, AVIRA seems to have reduced its false alarms rates (although it would be good if it would get even lower) and has earned the ADVANCED+ awards in nearly all tests. Due that, AVIRA got the annual award of overall winner of our tests of 2008.

BitDefender (**www.bitdefender.com**): BitDefender has good detection rates and good heuristics, but it still had some false alarms which lead to lower awards in the retrospective tests. BitDefender has a low impact on system performance and runs therefore quite light in the background.

eScan (**www.mwti.com**): eScan is a multi-engine product (based on the AVP engine). eScan did not get good results in the retrospective tests and also the detection rates in the on-demand tests are slightly winding down (but still good). In our opinion, eScan needs to considerably improve its heuristics engine.

ESET NOD32 (**www.eset.com**): ESET NOD32 Antivirus was product of the year for the last two years, but this year it placed a close second. ESET NOD32 has secured the ADVANCED+ award in both retrospective tests of 2008, due to its high proactive on-demand detection, and low false alarm rates. It also scored well in the overall on-demand detection tests (although it did not reach ADVANCED+ in the last on-demand test). ESET NOD32 Antivirus has a very low impact on system performance, but its detection rates leave some room for improvement (our internal observations indicate that ESET is moving in the right direction).

F-Secure (**www.f-secure.com**): F-Secure uses a variety of engines in its product. This gives F-Secure high results in the overall on-demand detection tests. F-Secure had in 2008 still a relatively big impact on system performance, but F-Secure is soon going to release an update which improves this considerably. F-Secure did also in 2008 not achieve very good results in the retrospective tests, but F-Secure includes various technologies to protect against new/unknown malware when files are executed.

GDATA (AVK) (**www.gdata.de**): GDATA AVK 2009 uses now the Avast and BitDefender engines. This combination brought to further improvements to the detection rates (even if it was already in the ~99% range), incl. better proactive detection. Also the impact on system performance improved further and is no longer such an issue as in past. A problem that seems to get worse and need to be addressed are the false alarms of the two used engines.

Kaspersky (**www.kaspersky.com**): Kaspersky shows good detection rates (earning ADVANCED+ awards in both on-demand tests) and its new heuristic shows very high proactive detection rates, although it still had some false alarms. Kaspersky uses technologies which lead to higher on-access scanning speeds over already scanned files, so that an users almost do not notice that Kaspersky is running in the background.

McAfee (**www.mcafee.com**): McAfee got three ADVANCED awards this year and had also the lowest false alarm rate of all tested products. Furthermore, McAfee's new in-the-cloud technology (Artemis) showed recently that it is able to reach very high detection rates while still maintaining a low false alarm rate.

Microsoft (**onecare.live.com**): Microsoft improved also in 2008, earning three ADVANCED awards. The generic detection signatures of Microsoft are quite good and Microsoft is also one of the products which had only very few false alarms compared to other vendors. In the second half of next year, Microsoft will discontinue OneCare and will offer a new no-cost antimalware solution, code-named "Morro", which we look forward to testing and expect the same if not better results.

Norman (www.norman.com): Norman got two ADVANCED awards in both on-demand detection tests, showing good detections rates. The scanner runs light in the background. Norman uses also a sandbox technology to identify new/unknown malware, but due to some false alarms Norman received only STANDARD awards this year in the retrospective tests.

Sophos (www.sophos.com): Sophos is an enterprise-focused security company which participated in our 2008 tests after being absent for some years. Sophos showed good detection rates (two ADVANCED awards in the on-demand tests) and also good proactive detection rates, but it did cause many false alarms (due to which Sophos did not get an award in the retrospective tests). Most of the false alarms were caused by Sophos's Suspicious File Detection option. This option is not enabled by default and blocks "suspicious" files, such as some shareware/freeware applications, which can then be authorized by administrators if required.

Symantec (www.symantec.com): Symantec (NAV) improved considerably even further in 2008 (esp. with the new 2009 version), reaching ADVANCED+ awards in both detection rate tests. The false alarm rates are low and the proactive detection rates are now also higher than in past (ADVANCED award in the latest retrospective test) due to its new improved heuristics. The on-demand scan speed is among the fastest, but the biggest improvement is the impact on system resources: Symantec runs now quite light on the system and has no big impact on the system performance.

TrustPort (www.trustport.com): TrustPort combines various Anti-Virus engines in its product which can be selected by the user. By default it uses usually mainly the AVG and Norman engines. Thanks to the various engines it uses, TrustPort had high overall on-demand detection rates and also high results in the retrospective tests, but it still has a relatively slow on-demand scanning speed and many false alarms. Also, the impact on system performance needs to be addressed.

VBA32 (www.anti-virus.by): VBA32 showed better results during 2008 (esp. detection rates) than in 2006. The product has a low impact on system performance and, in our opinion, a very easy to use user interface. VBA32 also has nice heuristics, but still some problems with false alarms. As a result, VBA32 got lower awards in the retrospective tests.

5. Copyright and Disclaimer

This publication is Copyright © 2008 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but no representative of AV-Comparatives e.V. can he held liable for the accuracy of the test results. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a Non-Profit Organization.

AV-Comparatives e.V. (December 2008)