

13 March 2008

By: Marius Oiaga, Technology News Editor

[The Best Windows Antivirus - 2008 Editions](#)

On Windows XP SP2

Security
Microsoft

The search for the best antivirus of 2008 has advanced one step further, courtesy of security solution testing lab [AV-Test.org](#). All the best available 2008 security suite editions were thrown against in excess of 1.1 million samples of malicious code on an arena of Windows XP SP2. At this point in time, with XP SP3 just around the corner, the results released by AV-Test are also valid for the third and final service pack of Windows XP, but not the same is valid for the Windows Vista (plus Service Pack 1) platform. "A comprehensive review should not only concentrate on detection scores of the on-demand scanner, as this would give a user only a very misleading and limited view of the product's capabilities," explained AV-Test's Andreas Marx as quoted by [Sunbelt Software](#). "The different detection types have to be taken together to make a valid statement about the whole detection mechanisms: neither static nor proactive detection mechanisms alone can catch all malware." Essentially, the tests run were designed to evaluate a wide range of the aspects that together build the puzzle of a bulletproof security solution. The antivirus programs had to deal with on-demand detection of malware samples, adware and spyware, but also of rootkits, and even the proactive detection capabilities for unknown malicious code. And on top of this, the analysis took into consideration factors like performance, the volume of false positives generated, response times, and cleaning capabilities. "It is important to have good heuristics, generic signatures and dynamic detection and prevention in place to be able to handle new unknown malware without any updates. It is crucial to have good response times, to be able to react to new malware, when proactive mechanisms fail to detect them. It is essential to have good static detection rates, to be able to handle already known malware, even before it is executed on a system. So comparing single features makes less sense, as we should think about the fact that a user has not bought an AV product to find some viruses and report them, but he has actually bought a service to keep his system malware-free," Marx added. The rankings with the best Windows antivirus for this year, considering just the 2008 editions that were tested by AV-Test, and in terms of malware, adware and spyware detection, have WebWasher-GW (with detection rates for malware of 99.85% and for adware and spyware of 99.86%), AVK (G Data) (99.91% - 99.85%), TrustPort (99.63% - 99.82%) and AntiVir (Avira) (99.32% - 99.15%) in the first four positions. The list continues with the remaining antivirus tested out of the total 30 security solutions. The detection rates for malware, as well as adware and spyware are for Trend Micro 98.72% - 95.14%; Sophos 98.10% - 98.83%; Nod32 (Eset) 97.85% - 96.33%; Microsoft 97.79% - 91.50%; BitDefender 97.77% - 98.77%; Kaspersky 97.17% - 92.02%; Norton (Symantec) 95.70% - 98.62%; Panda 95.62% - 95.57%; McAfee 95.58% - 98.56% etc. Sophos was quick to celebrate its victory over rivals Symantec and McAfee. "Sophos continues to innovate and improve the techniques used to protect against viruses, Trojans, spyware, adware and other threats. It's particularly gratifying to see Sophos praised for being 'very good' at detecting unknown malware," said Guy Edsall, product manager at Sophos. "Sophos received high scores across the board. Combining these excellent protection capabilities with Sophos's underlying philosophy of simple management has been the driver behind many companies switching from Symantec and McAfee to Sophos." The results for the Anti-virus comparison test of current anti-malware products, March 2008, are available via Sunbelt Software [here](#), [here](#), and [here](#). With the original Excel spreadsheet from AV-Test up for grabs [here](#).