

Symantec vs. Trend Micro Comparative Aug. 2009



On-demand Detection of Malicious Software

Language: English

August 2009

Last Revision: 28th October 2009

www.av-comparatives.org

Tested Products



- Symantec Endpoint Protection
Small Business Edition

versus

- Trend Micro Worry Free Business Solution

Tested products

AV Comparatives tested Symantec's Endpoint Protection Small Business Edition 12 against Trend Micro's Worry-Free Business Solution 16. The testing included on demand tests and false positive tests.

For more information on the methodology the AV Comparatives methodology document at: <http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf>

- **Symantec's Endpoint Protection Small Business Edition 12**
- **Trend Micro's Worry-Free Business Solution 16**

All products were up to date to the 10th of September 2009 and have access to the internet.

Versions

Symantec

- Symantec Endpoint Protection Small Business Edition, 12.0.122.192

Trend Micro

- Worry Free Business Solution, Version: 16.0.1331

System

Operating System: Windows Vista 6.0.6002, Service Pack 2

Methodology

The testing methodology can be found at www.av-comparatives.org.

All four products have been tested with default settings, in the cloud technology was turned on.

Management Summary

What to Compare?

In this test we compared the on-demand detection capabilities of the products.

An on-demand scanner (as well as the on-access scanner) is often used by used to verify on a regular base that the PC is malware-free or used on an already infected system to discover and remove infections.

The on-demand detection rates show the baseline detection that a product provides. On-demand and on-access scanners using signatures and heuristics provide deterministic results (malware detected vs. not detected / clean) which do not need any high-level knowledge or input by the user, therefore can be used by anyone without problems.

Results

Reaching high detection rates at the cost of false alarms (giving an alert that a file is malicious while it is not) is easy, but good products need to have high/reliable detections without causing too many false alarms. False alarms can cause as much troubles as a real infection, including loss of time or even worse loss of productivity and data.

On-Demand

Symantec showed high detection rates (all over the 90% range) in all malware categories and a total coverage of around **98,3%**.

Trend Micro showed to lack detections in various malware categories, esp. in regard to Backdoors and Trojans (which are among the most prevalent malware types nowadays). The total detection rate reached by Trend Micro was **74,2%**.

False Positives

Symantec had only **5** false alarms compared to **11** false alarms of Trend Micro while scanning our set of clean files. Nevertheless, both products showed to not have high false alarm rates.

Results

On-Demand Test-Set Malware

The used test-set is Test-Set B (like used in the on-demand test of August 2009, which contains about 1.6 Millions of malware samples from ~January 2009 to ~August 2009. Detection Set B (Jan 2009 - Aug 2009)

	Samples	Symantec Endpoint Protection Small Business Edition		Trend Micro Worry-Free Business solution	
		detected	%	detected	%
Windows viruses	23,791	22,601	95,0%	18,023	75,8%
Macro viruses	1,198	1,198	100,0%	1,189	99,2%
Script malware	4,466	4,387	98,2%	3,995	89,5%
Worms	95,881	94,150	98,2%	81,873	85,4%
Backdoors/Bots	323,723	321,259	99,2%	230,998	71,4%
Trojans	1,084,602	1,065,831	98,3%	806,635	74,4%
other malware	28,431	26,577	93,5%	17,133	60,4%
TOTAL	1,562,092	1,536,003	98,3%	1,159,846	74,2%

On Demand Test Clean Files

False Positives

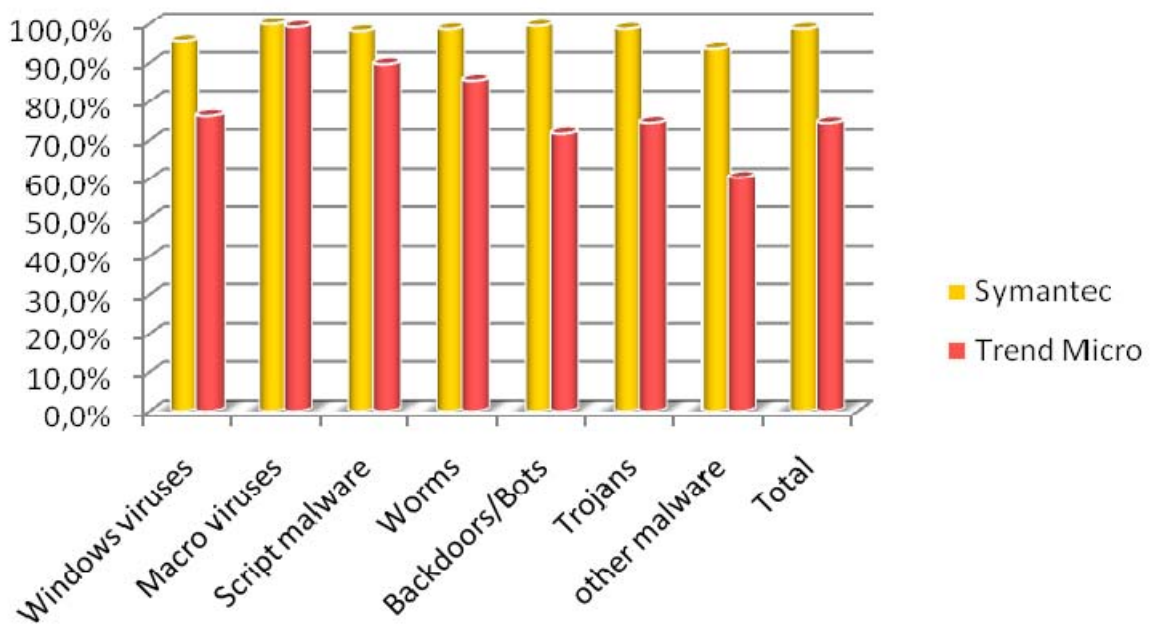
Symantec's Endpoint Protection Small Business Edition 12 **5** (few)

Trend Micro's Worry-Free Business Solution 16 **11** (few)

Graphics

On Demand Detection (higher is better)

Symantec's Endpoint Protection Small Business Edition 12
versus
Trend Micro's Worry-Free Business Solution 16

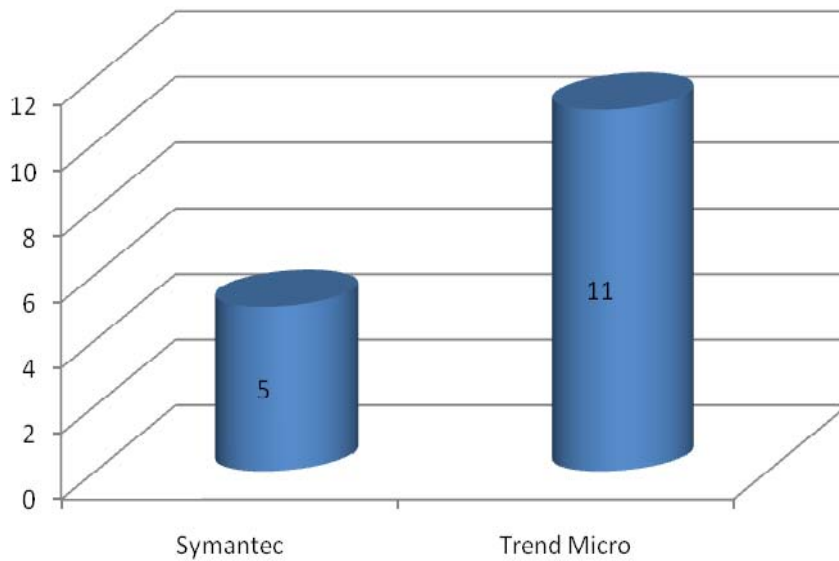


False Positives (lower is better)

Symantec's Endpoint Protection Small Business Edition 12
versus
Trend Micro's Worry-Free Business Solution 16

In order to better evaluate the quality of the detection capabilities of products, AV Comparatives also provided a false positive test. False positives can cause as much trouble as a real infection. Please consider the false positive rates when looking at competing products. The sample set used for the false positive test was exactly the same as that used in the August On-Demand Testing conducted by AV-Comparatives. See the report for more details at:

http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf



Copyright and Disclaimer

This publication is Copyright © 2009 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 a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. 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 registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (September 2009)