



# Trend Micro Endpoint Comparative Report Performed by AV-Test.org

---

*Results from December 2009*

## Executive Summary

---

In December of 2009, AV-Test.org performed endpoint security benchmark testing on five market-leading Enterprise endpoint solutions from Symantec, McAfee, Microsoft, Sophos and Trend Micro.

AV-Test.org tested zero-day attacks actually occurring in the wild by sourcing malicious URLs that had malware associated with them. The testing occurred simultaneously across all vendors' platforms to ensure no biases during the test runs. Products were configured to block or detect the threats at multiple levels, thereby giving each vendor maximum ability to protect against these threats.

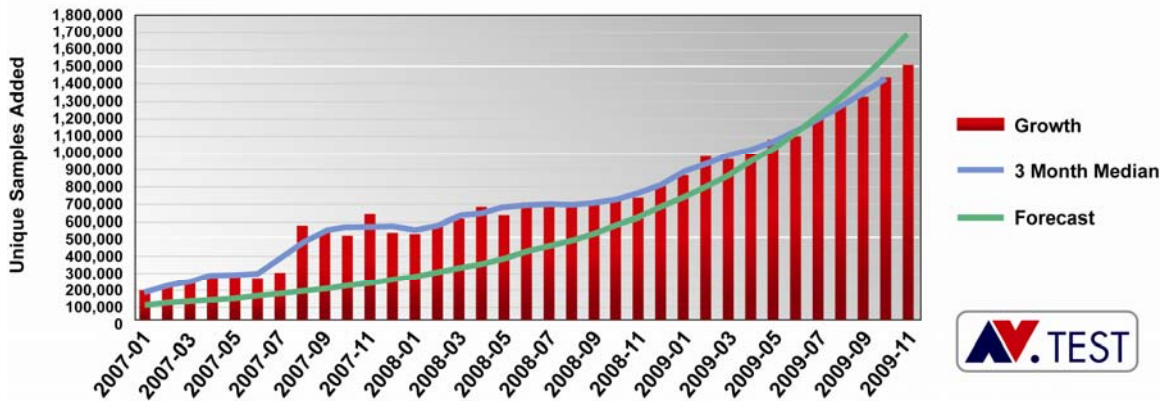
In these tests, Trend Micro emerged as the overall winner. Trend also demonstrated a decided advantage in blocking these threats at their source, the URL, with a significant contribution from Trend Micro™ Smart Protection Network™ and its Web reputation services. With an overall score at blocking zero-day threats of nearly 66 percent, the Trend Micro OfficeScan Client/Server Edition 10 (OfficeScan 10) stands distinctly apart from other products, whose averages ranged from just 38 to 59 percent.

## Overview

---

Traditionally, endpoint testing has been done by updating each product's signatures, removing the device from the network, and then copying a test set of malicious files onto the device to determine how many can be caught. That was fine when only a small number of malicious files were being introduced to the world, but today, according to the latest statistics from AV-Test.org, we're seeing over 1.5 million unique samples every month.

## New Unique Samples Added to AV-Test.org's Malware Collection



### Exposure Layer Detection and Blocking Reduces Risk

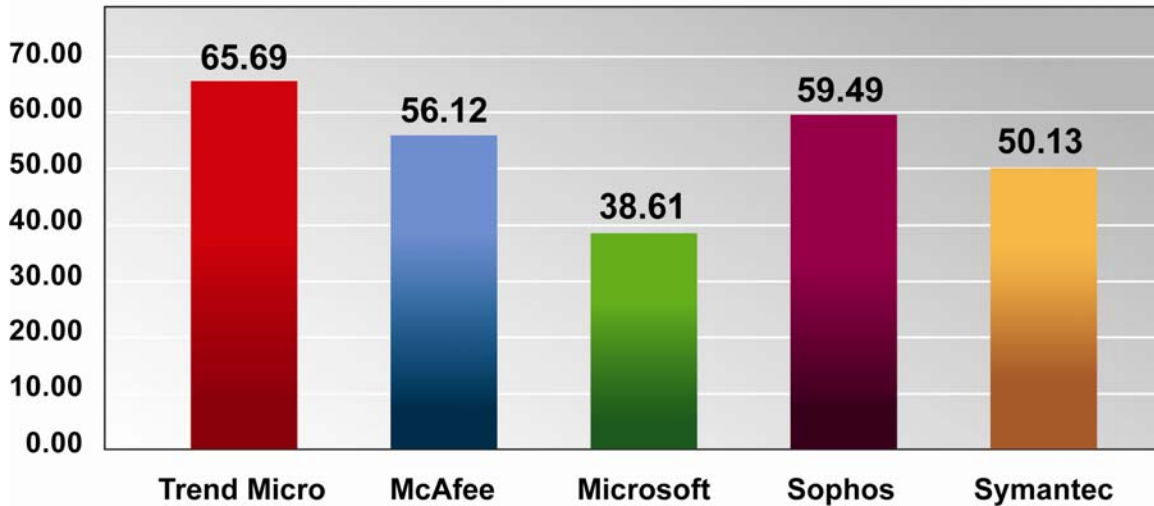
This “threat of volume” is creating issues for all vendors who attempt to keep up with these new emerging threats simply using file-based detection methods. File-based detection requires that each threat have an analogous signature file created and distributed by the antivirus company. Additionally, the majority of threats now come from the Internet (92% according to TrendLabs in 2008) via compromised webpages, BSEO (Blackhat Search Engine Optimization) and the use of social engineering. New technologies need to be used to combat these new threat vectors.

As such, Trend Micro commissioned AV-Test.org to perform a more real-world test of endpoint solutions that doesn't just score how well a product can detect file-based threats (Infection Layer), but includes the ability to block the threat at its source (Exposure Layer). The ability of a solution to source, analyze and block new threats that it cannot identify is becoming critical, due to the rapid rise in the amount of threats being released in the wild. Exposure Layer blocking reduces the risk to the network because fewer threats will impact network bandwidth, or require computing resources to block them at the endpoint. Another aspect of the test performed by AV-Test.org is retesting after 1 hour to determine if any vendors have added new protection for threats missed in the initial run (a.k.a. “Time to Protect”).

In December 2009, AV-Test.org tested five market-leading Enterprise endpoint solutions from Symantec, McAfee, Microsoft, Sophos and Trend Micro. Trend Micro emerged as the overall winner, with a decided advantage in both Exposure layer protection and time to protect.

As shown below, Trend Micro OfficeScan 10 ranked #1 in Overall Protection against these leading vendors in number of threats blocked.

## AV-Test.org Benchmark Test December 2009



### Products Tested

---

AV-Test.org tested the following five products during December 2009:

- Trend Micro OfficeScan Client/Server Edition 10
- Symantec Endpoint Protection v11
- Microsoft Forefront Client Security v1.5
- McAfee Total Protection for Endpoint with Artemis and SiteAdvisor
- Sophos Endpoint Security and Control v9.0.1

### Results and Analysis

---

Trend Micro OfficeScan 10, powered by the Smart Protection Network, which includes both Web reputation and File reputation capabilities, performed well at both the Exposure layer and the Infection Layer, allowing it to receive the top ranking among all solutions.

100% = Perfect Score for Each Metric	Trend Micro	McAfee	Microsoft	Sophos	Symantec
Exposure Layer	<b>65.1%</b>	16.07%	0%	59.26%	0%
Infection Layer	<b>50.46%</b>	64.48%	51.48%	51.79%	66.84%
Overall Score	<b>65.69%</b>	56.12%	38.61%	59.49%	50.13%

Trend Micro and Sophos appear to have the most robust technology to block threats at their source, thereby, ensuring no file is downloaded prior to detection. Symantec and Microsoft do not have any technology within the client portion of their Enterprise solutions capable of blocking threats coming from URLs at their source. They must wait to analyze the file during download or while writing to disk\*. McAfee does include SiteAdvisor to block malicious web pages, but for this test it did not have a good showing.

Symantec and McAfee performed the best at the Infection layer, which helped their overall score, but based on their Exposure Layer score it still appears they are focused on blocking threats using their file-based or signature-based detection methods. This could cause issues as more malicious files are released to the wild. Depending on file- and signature-based methods requires more work to create the signature files, distribute and update these files on each endpoint. As a result, the network and the endpoint computer resources will be increasingly used for protection, as threats multiply.

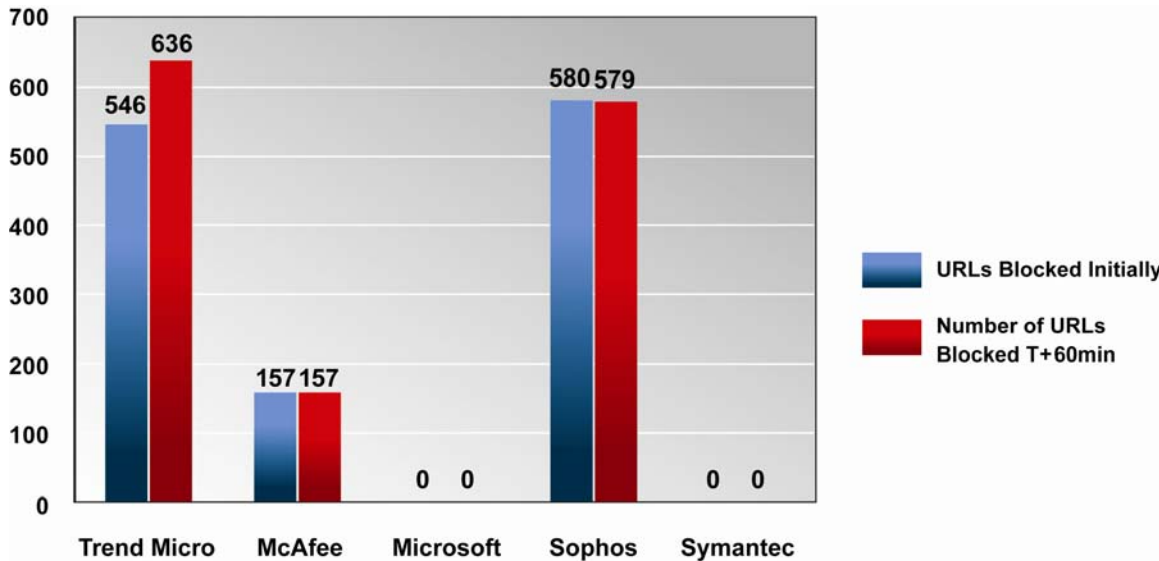
Overall, the scores are lower than you would normally see in many of today's tests. We think that is due to the fact that we tested Zero-day threats and the corpus of URLs and files were sourced very shortly prior to the test, thereby not allowing the vendors much time to obtain the samples.

Another aspect not widely known is that the underground cybercriminal industry provides services to developers for testing malicious files against the latest signatures from vendors. These tools buy the criminals have some time before their malicious files can be detected.

<http://www.wired.com/threatlevel/2009/12/virus-check/>

These issues require vendors to vastly improve their ability to source, analyze and block unknown threats. For this reason, the methodology utilized by AV-Test.org in this test by re-running the samples again after 1 hour. This gives vendors products a chance to find and block threats through feedback, analyze each of the URLs and files and ultimately provide protection

prior to the next run. The plus one-hour tests should have improved if feedback was well-used to improve protection. However, the scores were disappointing for all vendors, except for Trend Micro.



As shown, Trend Micro was able to block 90 additional URLs after 1 hour using the Smart Feedback component built into OfficeScan 10. No other vendor was able to add additional protection for unknown threats that went undetected.

On the Infection layer, no vendor was able to add any appreciable increases in detection for files not detected in the initial run. Trend Micro added detection for 2 additional files and Sophos added 1 file after 1 hour. Clearly, all vendors need improvement in this area.

## Rankings, Corpus, and Methodology

### Scoring and Rankings

The overall scores were derived by taking a weighted average from each layer (Exposure & Infection) in order to ensure each vendor was given credit regardless of which layer their products blocked each threat.

Note that these rankings do not consider performance, scalability, user interface, features, or functionality — only protection effectiveness against the December 2009 corpus.

## The Corpus

AV-Test.org compiled the corpus for testing by searching the Internet for malicious URLs that have associated malware. For this test they found 977 URLs and the associated 977 malicious files to conduct the test.

The URLs/files that AV-Test.org uses for testing are gathered from sites in the wild, using a variety of proprietary discovery, analysis, and verification techniques. They are neither supplied by, nor known to, any of the companies whose products were tested.

## Test Methodology

The test methodology adopted by AV-Test.org was developed together with Trend Micro and can be found within the following whitepaper.

[http://us.trendmicro.com/imperia/md/content/us/trendwatch/coretechnologies/wp01\\_benchmark\\_090922us.pdf?zid=nss\\_lp\\_benchmark\\_pdf](http://us.trendmicro.com/imperia/md/content/us/trendwatch/coretechnologies/wp01_benchmark_090922us.pdf?zid=nss_lp_benchmark_pdf)

## In Summary

Some conclusions we can make from the data presented here.

1. Vendors like Trend Micro that have invested in and provided solutions that block threats at multiple layers (Exposure & Infection) provide better overall security against the new threats propagating today. They improve protection by keeping threats completely off the network or computer using proactive technologies like Web reputation instead of waiting for malicious files to be downloaded.
2. Zero-day threats are more difficult to defend against, which is why the overall scores are lower than traditional detection rate tests, and why the Time to Protect factor has to be included in any real-world tests. This shows the effectiveness of a vendor at sourcing, analyzing and providing protection for any unknown threats.

*This comparative review, conducted independently by AV-Test.org in December 2009, was sponsored by Trend Micro. AV-Test.org aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab.*

\* Symantec and Microsoft do provide this type of protection in other products (gateway), but these were not used in this test.