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

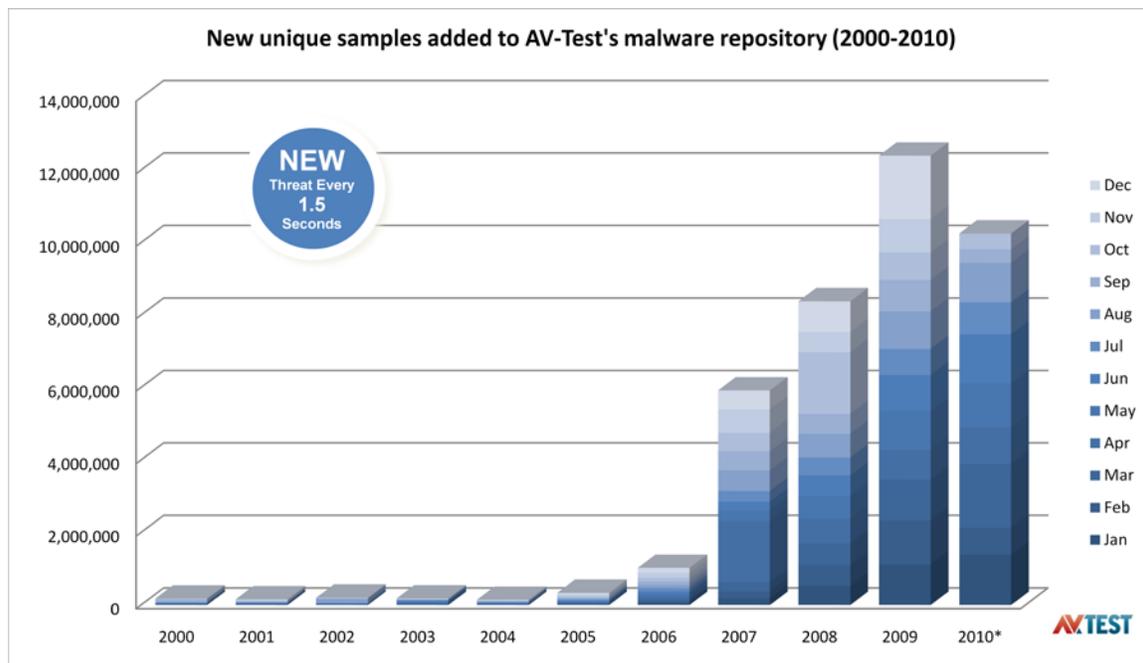*Results from October 2010*

Executive Summary

In October of 2010, 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 which have 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 clear overall winner blocking over 97% of the threats initially and 99% after 1 hour, a full 16% higher than the next competitor. Trend Micro also demonstrated a decided advantage in blocking these threats at their source, the URL, by blocking over 84% of the threats at this layer.

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's malware repository (2000-2010)

NEW
Threat Every
1.5
Seconds

Source: AV-Test.org
* November, December results not yet in

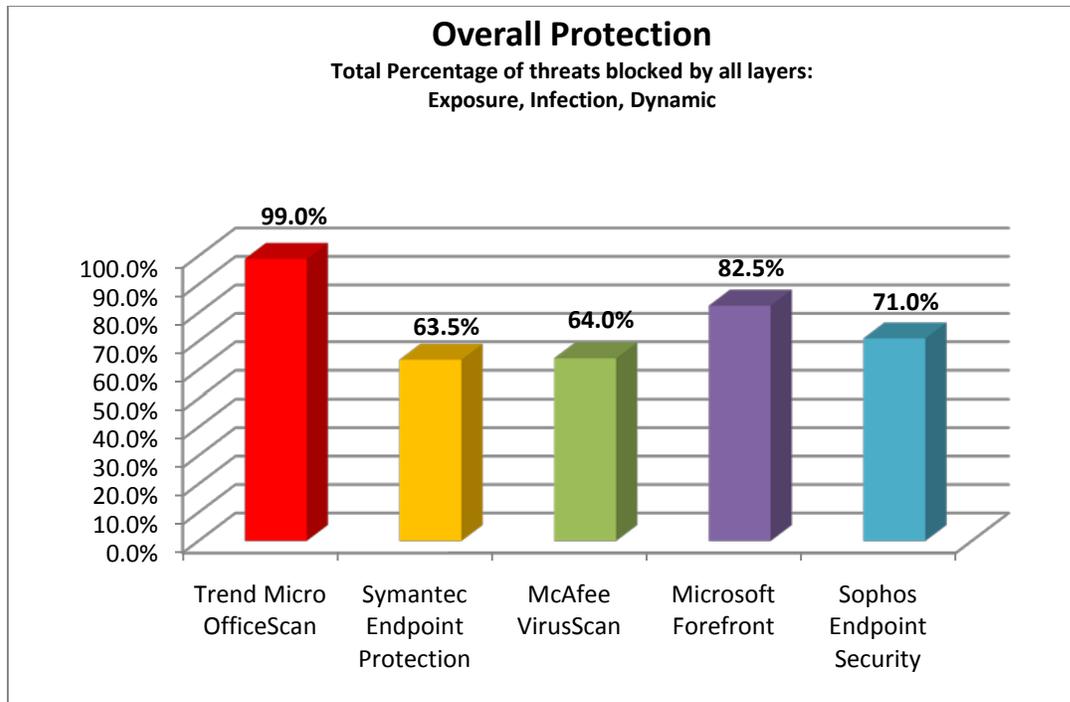**Exposure Layer Detection and Blocking Reduces Risk**

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 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, AV-Test.org performed 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) and detect/block the threat during execution (Dynamic 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. In this test, only threats that were not blocked by a previous layer were tested against the next layer, and so on. 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 October 2010, AV-Test.org tested five market-leading Enterprise endpoint solutions from Symantec, McAfee, Microsoft, Sophos and Trend Micro. The results of the test showed that

Trend Micro was the overall winner, with a decided advantage in both Exposure layer protection and time to protect.

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

Overall Protection
Total Percentage of threats blocked by all layers:
Exposure, Infection, Dynamic

Product	Percentage
Trend Micro OfficeScan	99.0%
Symantec Endpoint Protection	63.5%
McAfee VirusScan	64.0%
Microsoft Forefront	82.5%
Sophos Endpoint Security	71.0%

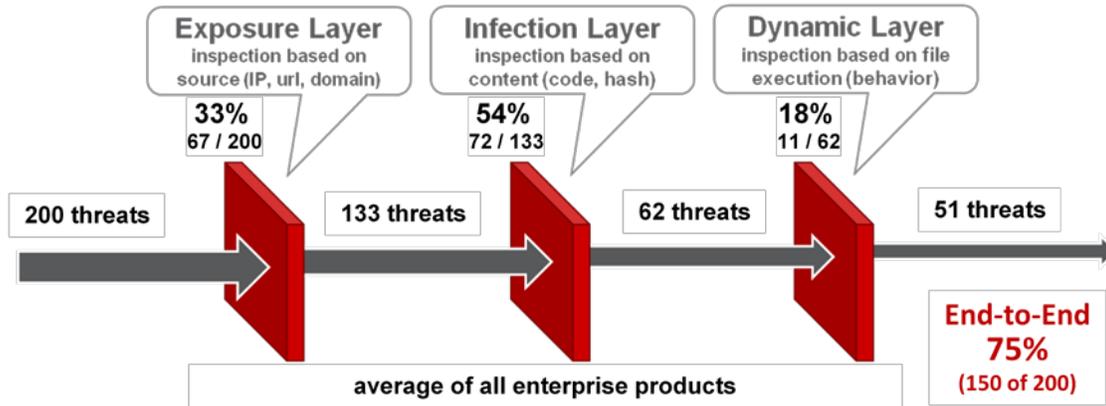Note: Results are based on the T+60 minute results

Products Tested

AV-Test.org tested the following five products during October 2010:

- Trend Micro OfficeScan v10.5.1083

- Symantec Endpoint Protection v12.0.1001.95

- McAfee VirusScan Enterprise v8.7.0.570

- Microsoft Forefront Client Security v1.5.1981.0

- Sophos Endpoint Security and Control v9.5.3

Results and Analysis

Trend Micro received the top rankings among all products.

Exposure Layer — inspection based on source (IP, url, domain)	Infection Layer — inspection based on content (code, hash)	Dynamic Layer — inspection based on file execution (behavior)
33% — 67 / 200	54% — 72 / 133	18% — 11 / 62

200 threats → 133 threats → 62 threats → 51 threats

average of all enterprise products

End-to-End 75% (150 of 200)

Threats prevented at each layer (of total threats that reached that layer)

	Trend Micro	Microsoft	Sophos	McAfee	Symantec
Exposure Layer	85% (169 of 200)	2% (4 of 200)	61% (122 of 200)	7% (14 of 200)	0% (0 of 200)
Infection Layer	68% (21 of 31)	82% (161 of 196)	24% (19 of 78)	51% (94 of 186)	54% (107 of 200)
Dynamic Layer	80% (8 of 10)	0% (0 of 35)	2% (1 of 59)	22% (20 of 92)	22% (20 of 93)
All Layers	99% (198 of 200)	83% (165 of 200)	71% (142 of 200)	64% (128 of 200)	64% (127 of 200)

Note: Results are based on the T+60 minutes result. Prevention percentages at each layer do not add up to overall score. For example, with Trend Micro OfficeScan: Exposure layer prevented 169 of 200 threats (85%); Infection layer prevented 21 of 31 threats (68%); Dynamic layer prevented 8 of 10 threats; Overall prevented 198 of 200 threats (99%).
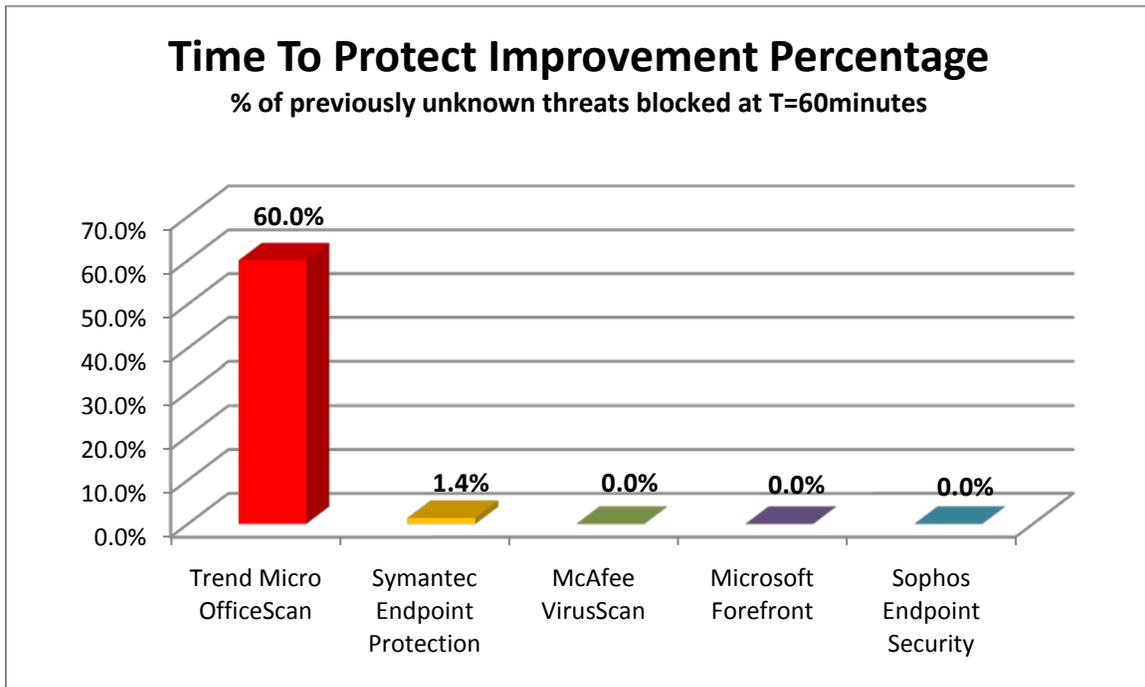
Trend Micro appears to have the most robust technology to block threats at their source (23.5% higher than closest competitor), thereby, ensuring no file is downloaded prior to detection. This ensures these threats do not require bandwidth to download them, nor does the threat need to use computer resources to identify or execute the malicious code.

Microsoft performed the best at the Infection layer, which helped their overall score, but also with a low Exposure score means they are still focused on blocking threats using their signature-based or behavior-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. This may be due to the fact that 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 through the normal industry sharing process.

The amount of threats today requires vendors to improve their ability to source, analyze and block unknown threats. For this reason, the methodology utilized by AV-Test.org in this test is to re-run the samples again after 1 hour. This gives vendors products a chance to automatically source the threats which bypassed their technologies in the first run, 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 the products have built in automation to manage this process.

Time To Protect Improvement Percentage
% of previously unknown threats blocked at T=60minutes

Vendor	Percentage
Trend Micro OfficeScan	60.0%
Symantec Endpoint Protection	1.4%
McAfee VirusScan	0.0%
Microsoft Forefront	0.0%
Sophos Endpoint Security	0.0%

NOTE: Time-to-protect improvement is the percentage of threats missed at T=0min that are subsequently prevented at T=60min. For example, with Trend Micro OfficeScan: At T=0min, 195 threats were prevented while 5 threats were missed. Of the 5 threats missed at T=0min, 3 were prevented at T=60min (3 of 5 equals 60%).

Trend Micro again proved it does an excellent job in this area with OfficeScan improving 60% from the first test run. The other vendors averaged 0.35% improvement. This means that of the total number of threats undetected during the first run, 60% of them were blocked during the T+60 run.

Rankings, Corpus, and Methodology

Scoring and Rankings

The overall scores were derived by adding up the total number of threats blocked by each solution, regardless of which layer blocked it.

Note that these rankings do not consider performance, scalability, user interface, features, or functionality — only protection effectiveness against the October 2010 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 sourced 200 malicious URL samples and the associated 200 malicious file samples 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 can be found at the following webpage.
http://www.av-test.org/services_and_testing

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 & Dynamic) 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 previously unobserved threats.

This comparative review, conducted independently by AV-Test.org in October 2010, 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.