Real World Corporate Endpoint Test Report

A test commissioned by Trend Micro and performed by AV-Test GmbH

Executive Summary

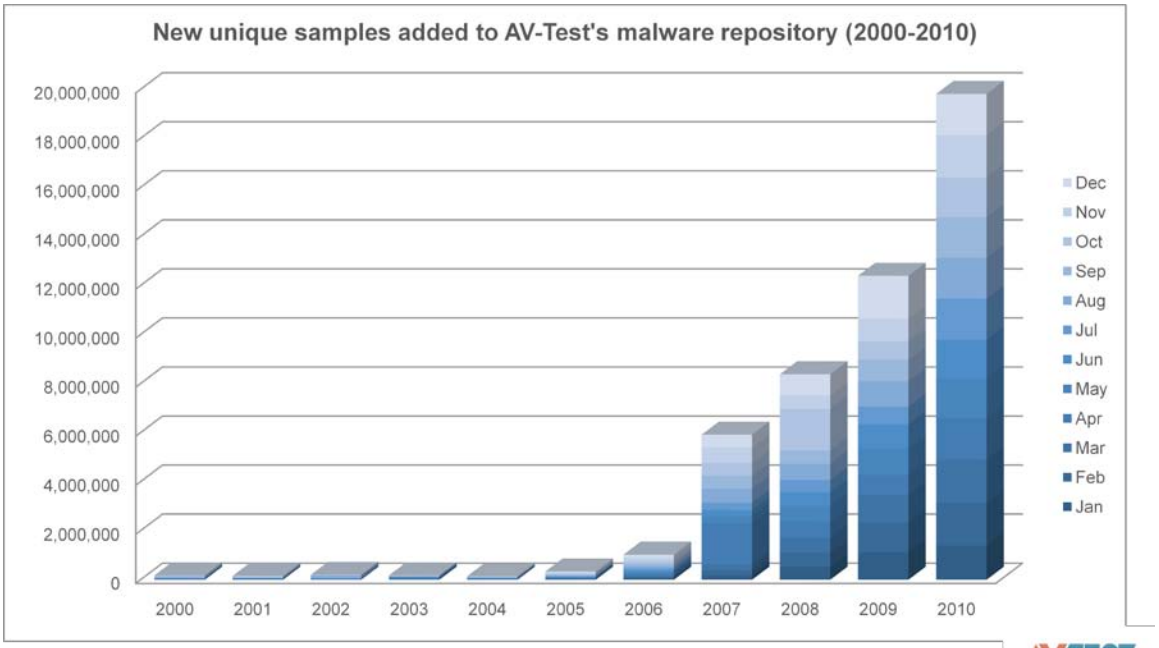
In January 2011, AV-Test.org performed endpoint security benchmark testing on five market-leading Enterprise endpoint solutions from Symantec, McAfee, Microsoft, Sophos and Trend Micro.

AV-Test.org tested zero-day attacks actually occurring in the wild by sourcing 200 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 given the opportunity to block or detect the threats at multiple levels, thereby giving each vendor maximum ability to protect against these threats. Cloud-based protection components were enabled for all products if not activated by default. This includes features like Trend Micro's web reputation service.

In this test, Trend Micro emerged as the clear overall winner blocking over 99.5% of the threats initially and 100% after 1 hour, a full 23 percentage points higher than the next competitor. Trend Micro also demonstrated a decided advantage in blocking these threats at their source, the URL, by blocking over 97% of the threats at this layer. Note: Test results can vary over time and may vary with other configuration settings.

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, they saw 19 million unique samples in 2010.



Source: AV-TEST

Exposure Layer Detection and Blocking Reduces Risk

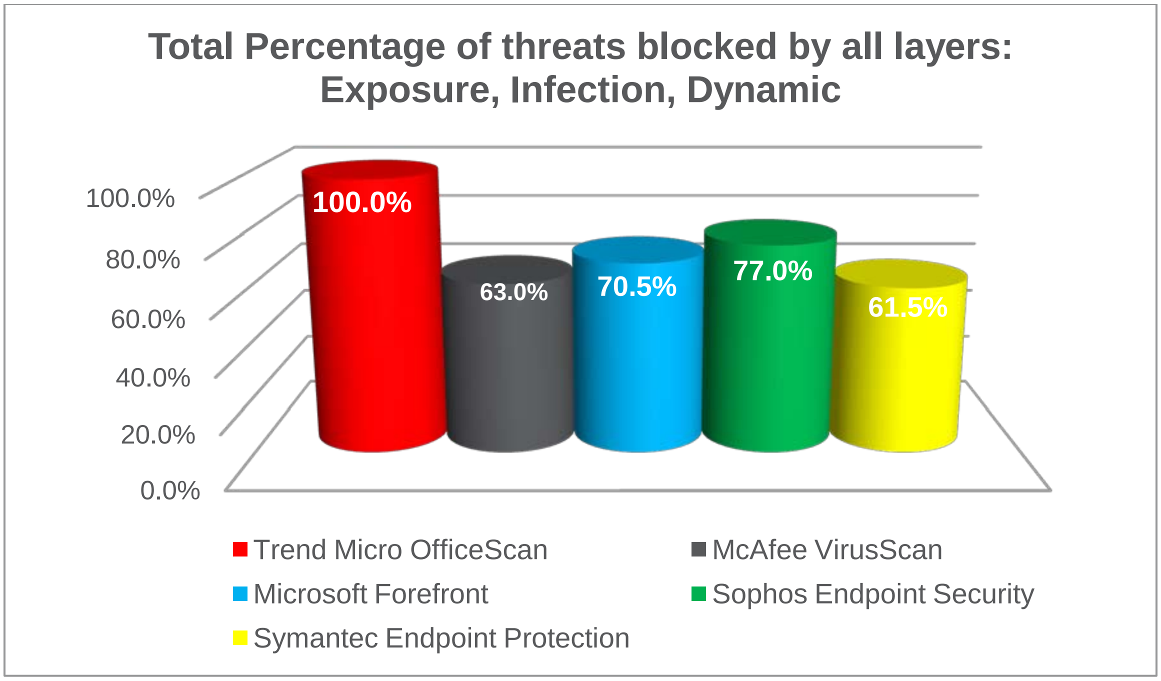
This “threat of volume” created issues for all vendors in order to keep up with these new emerging threats by simply using file-based detection methods. File-based detection requires that each threat have an analogous signature file created and distributed by the antivirus company. Additionally, the majority of threats now come from the Internet via compromised webpages, BSEO (Blackhat Search Engine Optimization) and the use of social engineering. Vendors have deployed new technologies to combat these new threat vectors such as blocking the URL source of malware drive-by downloads.

As a result, 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, identify and protect against new threats that it cannot detect is becoming critical, due to the rapid rise in the number 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 scan and detect 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 the same threats 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 January 2011, 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 across all three layers of protection.



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

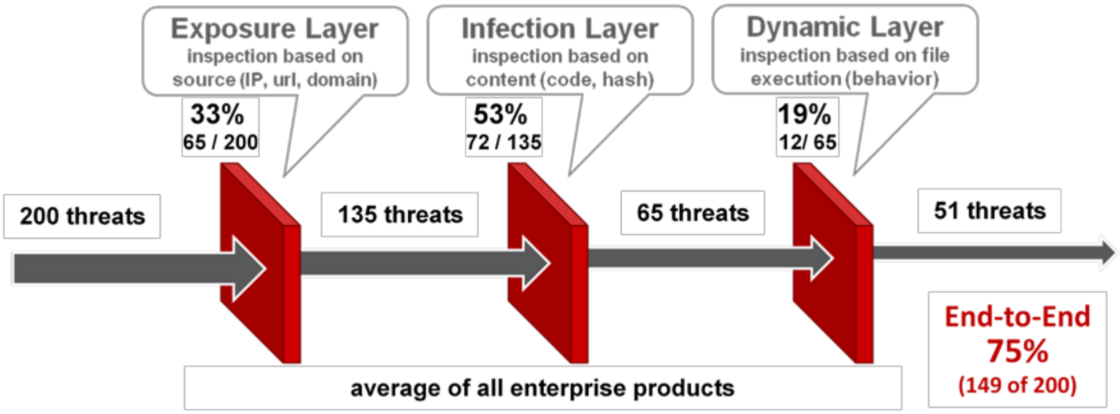
Products Tested

AV-Test.org tested the following five products during January 2011:

- Trend Micro OfficeScan v10.5.1161
- Symantec Endpoint Protection v12.0.1001.95
- McAfee VirusScan Enterprise v8.7.0.570
- Microsoft Forefront Client Security v2.0.657.0
- Sophos Endpoint Security and Control v9.5.5

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%
65 / 200
53%
72 / 135
19%
12/ 65
200 threats
135 threats
65 threats
51 threats
End-to-End
75%
(149 of 200)
average of all enterprise products

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

	Trend Micro	Microsoft	Sophos	McAfee	Symantec
Exposure Layer	97% (194 of 200)	2% (3 of 200)	63% (126 of 200)	1% (2 of 200)	0% (0 of 200)
Infection Layer	67% (4 of 6)	68% (134 of 197)	19% (14 of 74)	50% (99 of 198)	54% (108 of 200)
Dynamic Layer	100% (2 of 2)	6% (4 of 63)	23% (14 of 60)	25% (25 of 99)	16% (15 of 92)
All Layers	100% (200 of 200)	71% (141 of 200)	77% (154 of 200)	63% (126 of 200)	62% (123 of 200)

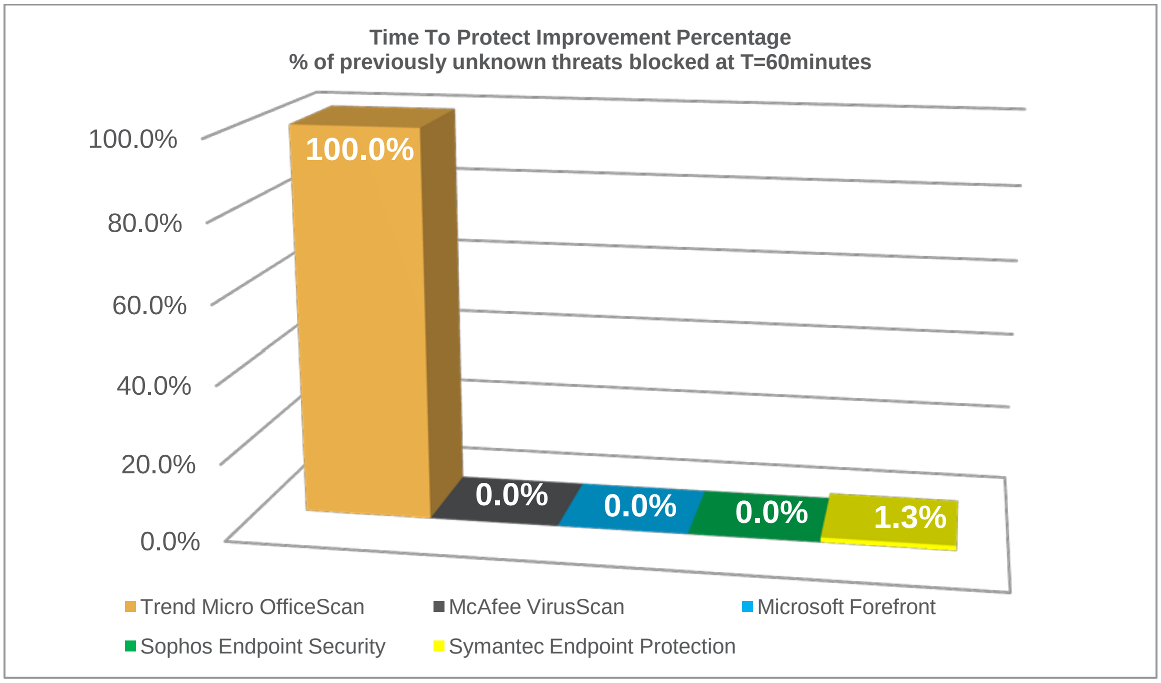
Note: Results are based on the T+60 minutes result. Prevention percentages at each layer do not add up to overall score. For example, with Trend Micro OfficeScan: Exposure layer prevented 194 of 200 threats (97%); Infection layer prevented 4 of 6 threats (67%); Dynamic layer prevented 2 of 2 threats (100%); Overall prevented 200 of 200 threats (100%).

Trend Micro appears to have the most robust technology to block threats at their source (34 percentage points 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 their low Exposure score means they are still focused on blocking threats using 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.

Besides Trend Micro's score, 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, identify and protect against 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.



NOTE: Time-to-protect improvement is the percentage of threats missed at T=0min that are subsequently prevented at T=60min. For example, with Symantec Endpoint Protection: At T=0min, 122 threats were prevented while 78 threat was missed. Of the 78 threat missed at T=0min, 1 was prevented at T=60min (1 of 78 equals 1.3%). In contrast, Trend Micro prevented 199 threats and missed 1 at T=0min which it subsequently prevented at T=60min (1 of 1 equals 100%).

Trend Micro again proved it does an excellent job in this area with OfficeScan improving 100% from the first test run. The other vendors averaged 0.325% improvement.

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 January 2011 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 previously disclosed 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 January 2011, 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.