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

Results from October 2010
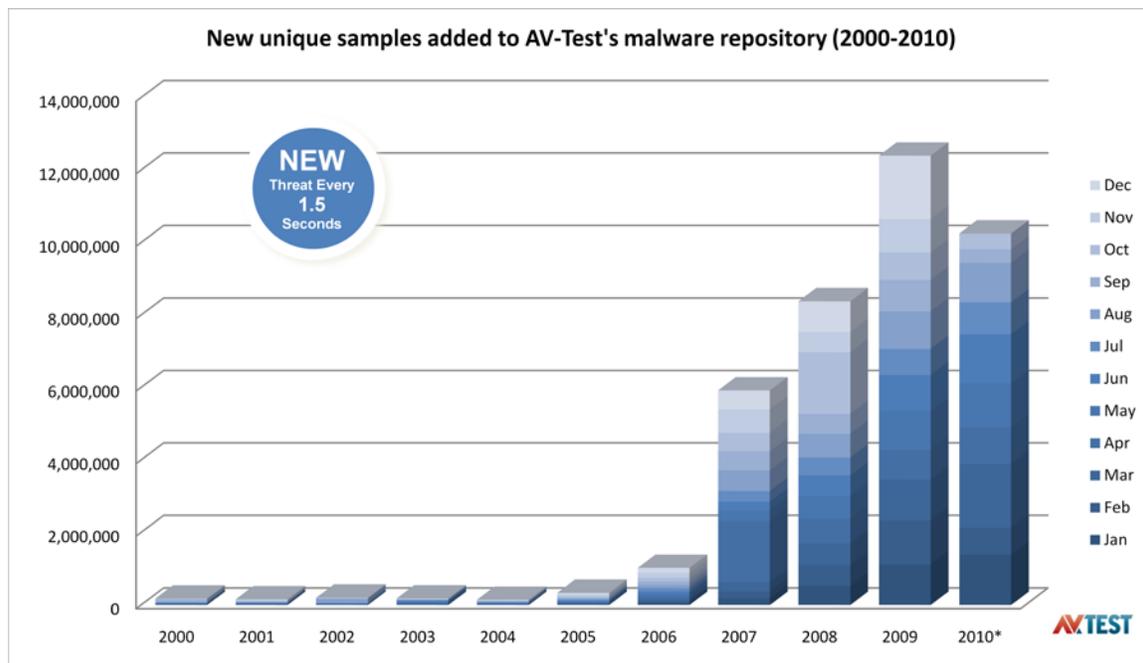
Executive Summary

In October of 2010, AV-Test.org performed endpoint security benchmark testing on five market-leading SMB endpoint solutions from Symantec, McAfee, ESET, Kaspersky 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 Worry-Free Business Security v7 emerged as the clear overall winner blocking over 93% of the threats initially and 96% after 1 hour, a full 18% higher than the next competitor. Trend Micro also demonstrated a decided advantage in blocking these threats at their source, the URL by blocking over 90% of the threats.

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)

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

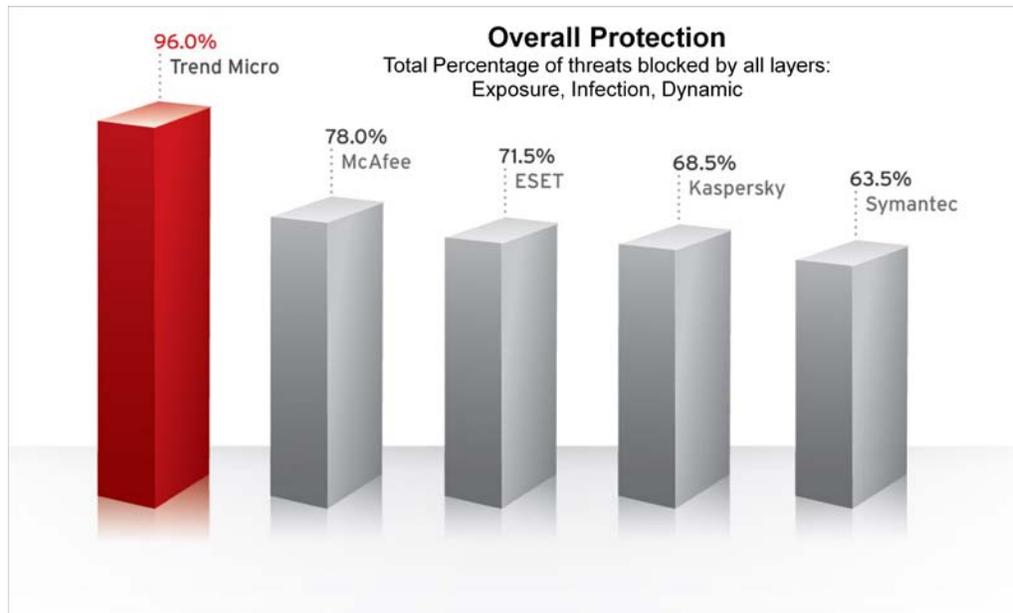**Exposure Layer Detection and Blocking Reduces Risk**

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 Small Business endpoint solutions from Symantec, McAfee, ESET, Kaspersky 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 Worry-Free Business Security 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

96.0% Trend Micro

78.0% McAfee

71.5% ESET

68.5% Kaspersky

63.5% Symantec

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 Worry-Free Business Security v7.0.1553
- Symantec Endpoint Protection Small Business Edition v12.0.1001.95
- McAfee SaaS Total Protection v5.2.0
- ESET Smart Security 4 Business Edition v4.2.64.12
- Kaspersky Anti-Virus 6.0 for Windows Workstations v6.0.4.1442a

Results and Analysis

Trend Micro received the top rankings among all products.
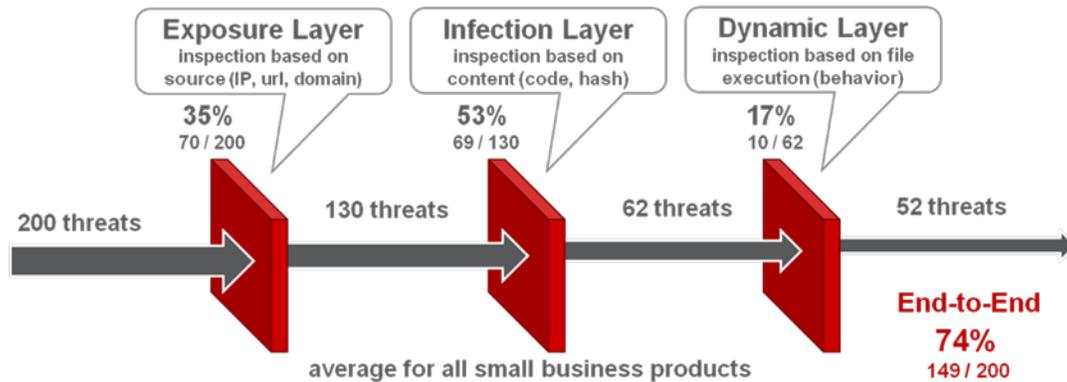
Threats prevented at each layer (of total threats that reached that layer)

	Trend Micro	McAfee	ESET	Kaspersky	Symantec
Exposure Layer	90% (180 of 200)	43% (86 of 200)	7% (13 of 200)	46% (91 of 200)	0% (0 of 200)
Infection Layer	60% (12 of 20)	61% (70 of 114)	62% (115 of 187)	27% (29 of 109)	54% (107 of 200)
Dynamic Layer	0% (0 of 8)	0% (0 of 44)	21% (15 of 72)	21% (17 of 80)	22% (20 of 93)
All Layers	96% (192 of 200)	78% (156 of 200)	72% (143 of 200)	69% (137 of 200)	64% (127 of 200)

NOTE: Prevention percentages at each layer do not add up to overall score. For example, with Trend Micro WFBS: Exposure layer prevented 180 of 200 threats (90%); Infection layer prevented 12 of 20 threats (60%); Dynamic layer prevented 0 of 3 threats; Overall prevented 192 of 200 threats (96%).
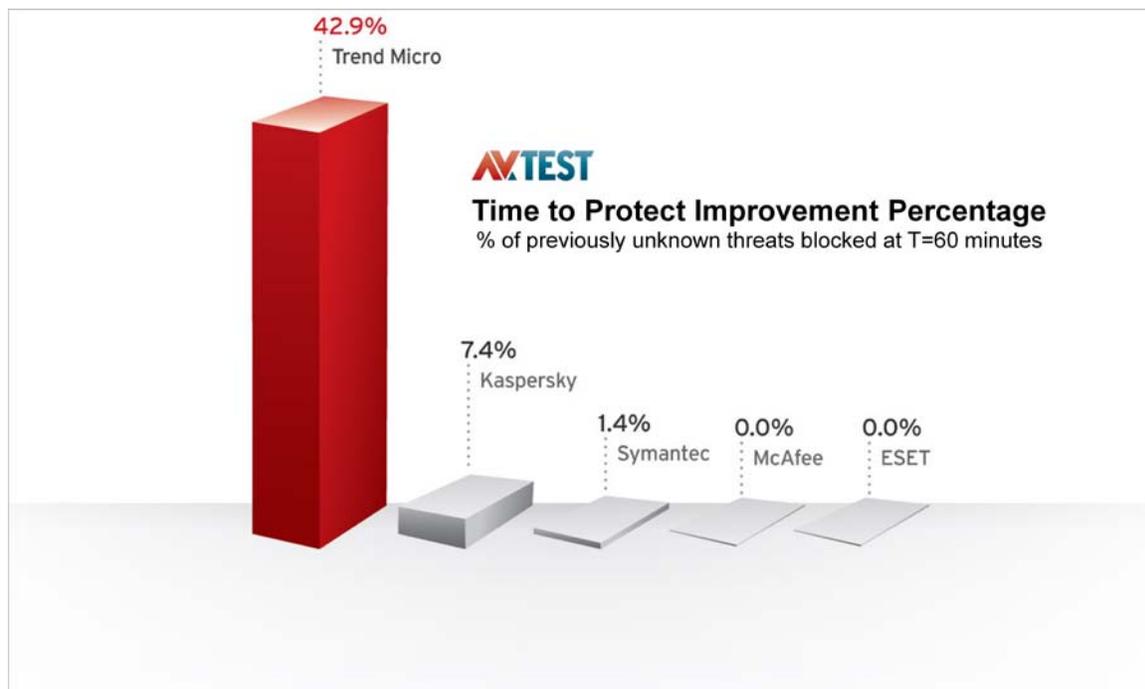
Trend Micro appears to have the most robust technology to block threats at their source (44% higher than closest competitor), thereby, ensuring no file is downloaded prior to detection. This ensures these threats do not require bandwidth to download them, nor does the threat need to be detected at the machine layer, meaning this threat never entered the PC or network.

ESET, McAfee & Trend Micro performed similar at the Infection layer, but as seen above, the number of files requiring scanning is different for each vendor. This could cause issues as more malicious files are released to the wild and not blocked at the Exposure layer. Also, 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. At the Dynamic layer,

Symantec scored the best, but also scanned the most files due to less protection at the previous two layers.

Overall, the scores are lower than you would normally see in many of today's file-based 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.

AV TEST

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

42.9%
Trend Micro

7.4%
Kaspersky

1.4%
Symantec

0.0%
McAfee

0.0%
ESET

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 WFBS 7: At T=0min, 186 threats were prevented while 14 threats were missed. Of the 14 threats missed at T=0min, 6 were prevented at T=60min (6 of 14 equals 42.9%).

Trend Micro again proved it does an excellent job in this area with Worry-Free Business Security improving 42.9% from the first test run. The other vendors averaged 2.2% improvement. This means that of the total number of threats undetected during the first run, 42.9% 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.